ISSN 2225-5435

Вестник УрФО

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 1(27) / 2018

УЧРЕДИТЕЛИ

ФГБОУ ВПО «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ООО «ЮЖНО-УРАЛЬСКИЙ ЮРИДИЧЕСКИЙ ВЕСТНИК»

ГЛАВНЫЙ РЕДАКТОР

ШЕСТАКОВ А. Л.,
д. т. н., профессор, ректор ФГАОУ ВО «ЮУрГУ (НИУ)» (г. Челябинск)

ОТВЕТСТВЕННЫЙ РЕДАКТОР

РАДИОНОВ А. А.,
д. т. н., профессор, проректор ФГАОУ ВО «ЮУрГУ (НИУ)» (г. Челябинск)

ВЫПУСКАЮЩИЙ РЕДАКТОР

СОГРИН Е. К.

ВЁРСТКА

ШРЕЙБЕР. А. Е.

КОРРЕКТОР

ФЁДОРОВ. В. С.

Журнал «Вестник УрФО. Безопасность в информационной сфере» включен в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени доктора и кандидата наук

Подписной индекс 73852 в каталоге «Почта России»

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Свидетельство ПИ № ФС77-65765 от 20.05.2016

Издатель: **ООО «Южно-Уральский юридический вестник»**

Адрес редакции и издателя: Россия, 454080, г. Челябинск, пр. Ленина, д. 76.
Тел./факс (351) 267-97-01.

Электронная версия журнала в Интернете:
www.info-secur.ru,
e-mail: urvest@mail.ru

16+

ISSN 2225-5435

UrFR Newslette
INFORMATION SECURITY
№ 1(27) / 2018

FOUNDER

SOUTH URAL STATE UNIVERSITY

SOUTH URAL LEGAL NEWSLETTER

CHIEF EDITOR

SHESTAKOV A. L.,
doctor of Technical Sciences, Professor, Rector South Ural State University, (Chelyabinsk)

MANAGING EDITOR

RADIONOV A. A.,
Doctor of Technical Sciences, Professor, Vice-Rector South Ural State University, (Chelyabinsk

PRODUCING EDITOR

SOGRIN E. K.

LAYOUT

SHRABER. A. E.

PROOFREADING

FEDOROV. V. S.

The journal « UrFR Newsletter. Information Security » is included in the List peer-reviewed scientific publications, in which should be published main scientific results of scientific dissertations degree of doctor and candidate of science

Subscription index 73852

in the «Russian Post» catalog

The journal is registered by the Federal service in the field of communication, information technology and mass communications.

Certificate
PI No. ФС77-65765 dd. 05/20/2016

Publisher: OOO « South Ural Legal Newsletter»

Editorial and publisher address: Russia, 454080, Chelyabinsk, Lenin Avenue, 76
Phone / fax (351) 267-97-01.

Electronic version of the magazine in the Internet:

www.info-secur.ru,
e-mail: urvest@mail.ru

16+

В НОМЕРЕ

IN THIS ISSUE

УДК 004.048 + 004.032.26 Вестник УрФО № 1(27) / 2018, с. 5–9

Асяев Г. Д., Рагозин А. Н.

АУТЕНТИФИКАЦИЯ ПО КЛАВИАТУРНОМУ ПОЧЕРКУ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННОЙ СЕТИ

В статье проведено исследование применения разновидностей нейронной сети для распознавания образов. Выявлена основная методика обучения нейронной сети. Определён минимальный набор входных данных для корректной аутентификации. Были проведены эксперименты, в ходе которого была выбрана наиболее оптимальная модель нейронной сети, которая с наименьшим количеством ошибок выполняла аутентификацию по клавиатурному почерку.

***Ключевые слова**: информация, аутентификация, нейронная сеть, клавиатурный почерк, биометрическая характеристика.*

Asyaev G. D., Ragozin A. N.

AUTHENTICATION KEYBOARD HANDWRITING USING A NEURAL NETWORK

In the article, the application of varieties of a neural network for image recognition has been studied. The main technique of neural network training is revealed. A minimal set of input data for correct authentication is defined. Experiments were carried out, during which the most optimal model of a neural network was chosen, which with the least number of errors performed keyboard-based authentication.

Keywords: *Information, authentication, neural network, keyboard handwriting, biometric characteristic.*

Рассматриваемая статья является продолжением ранее опубликованной работы [2]. В предыдущей работе определены основные виды нейронных сетей, которые могут применяться для аутентификации по клавиатурному почерку, рассмотрен их основной алгоритм, а также экспериментально определён минимальный набор входных данных. В настоящей работе выявлена методика и параметры обучения рассмотренных ранее нейрон-

ных сетей, проведено исследование зависимости временного интервала между нажатиями клавиш в различное время суток, а также экспериментально определена нейронная сеть, которая оптимальных образом решает задачу аутентификации по заданным требованиям. Идентификация личности является неотъемлемой частью любой политики информационной безопасности. Это сделать можно как при помощи традиционной парольной защиты, так и про помощи проверки физических и психофизических параметров человека. Однако большинство методов защиты очень часто подделываются злоумышленником, что может нанести существенный вред защищаемой информации (модификация, уничтожение, распространение), нарушая 3 составляющие информации:

- целостность;
- доступность;
- конфиденциальность.

Применение биометрических характеристик для аутентификации обладает высокой надёжностью ко взломам. В данной статье рассмотрена биометрическая система аутентификации, анализирующая динамический образ, который в свою очередь построен на анализе клавиатурного почерка.

Основными задачами исследования является:

1) определение эффективности применения нейронной сети для аутентификации по клавиатурному почерку;

2) определение минимального набора входных данных для корректной задачи аутентификации;

3) выбор наиболее оптимального типа нейронной сети для проведения процедуры аутентификации.

Рассмотрим алгоритм действия динамической биометрической системы:

1. С помощью регистрирующего технического устройства происходит процесс записи биометрической характеристики человека.

2. Повторяем первый этап несколько раз, как правило, от 3–5 раз.

3. Выделение в полученных шаблонах, уникальных биометрических идентификаторов.

4. Формирование базы данных этих идентификаторов [2].

5. При предъявлении регистрирующему техническому устройству биометрической характеристики, система выделяет уникальные идентификаторы [2].

6. Сравнение полученных данных с шаблоном, который хранится в базе данных.

7. Если уровень доверия превышает конкретный порог, то система успешно распознает пользователя и предоставляет требуемый ресурсы. При несоответствии уровня доверия, система блокирует доступ к запрашиваемым ресурсам [2].

В ходе выполнения исследования было усовершенствовано разработанное ранее программное обеспечение, которое регистрирует временной интервал между нажатиями клавиш, количество ошибок и высчитывает динамику ввода. В качестве парольной фразы выступали как не связанные по смыслу словосочетания (20–42 символов), так и произвольно генерируемый текст (для того чтобы исключить запоминание парольной фразы).

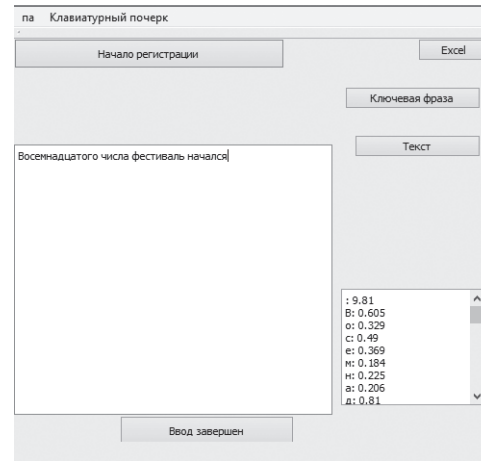


Рис. 1. Разработанное ПО

В ходе проведённого исследования было выявлено время суток, когда пользователь печатает максимально быстро. Было выбрано 5 пользователей с разными навыками печатания клавиатуры, которые на протяжении недели печатали текст длиной 50 символов. Экспериментально выявлено, что человек наиболее быстро печатает днём, и заметно медленнее вечером.

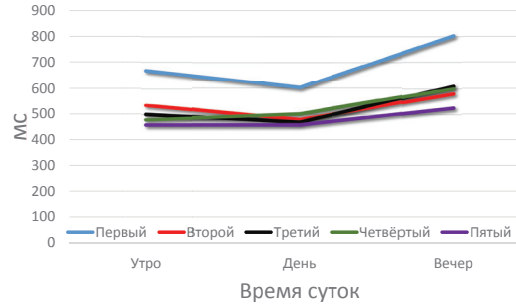


Рис. 2. Динамика изменения временного интервала между нажатиями клавиш в разное время суток

В ходе исследования рассматривались следующие типы нейронной сети:

1) нейронная сеть с прямым распространением сигнала и обратным распространением ошибки;

2) иерархическая сеть;

3) нейронная сеть Кохонена;

4) нейронная сеть, у которой количество входных слоёв прямо пропорционально количеству выходных.

Для корректного обучения требовалось не менее 10–15 выборок временного интервала для каждого пользователя. Для того, чтобы обучить сеть нужно подготовить обучающие данные. В нашем случае, тренировочные данные состоят из входных параметров – временного интервала каждого пользователя и желаемого результата (порядковый номер пользователя). В качестве данных для проверки предоставлялись три временных интервала между нажатиями клавиш для каждого из пользователей.

Нейронная сеть с прямым распространением сигнала и обратным распространением ошибки. Количество итераций было выбрано 14 для получения оптимального результата. Из рисунки ниже видно, что обучение остановилось при минимальном значении квадрата ошибки. На рисунке показано изменение коэффициента градиента по отношению к числу эпох. Конечное значение градиентного коэффициента при количестве эпох равное 14 составило 0,0021282, что приближено к нулю. Минимальным значением коэффициента градиента будет обучение и тестирование сетей. Из рисунка видно, что значение градиента уменьшается с увеличением числа эпох. Mu – контрольный параметр для алгоритма, используемого для обучения нейронной сети. Выбор mu напрямую влияет на конвергенцию ошибок.

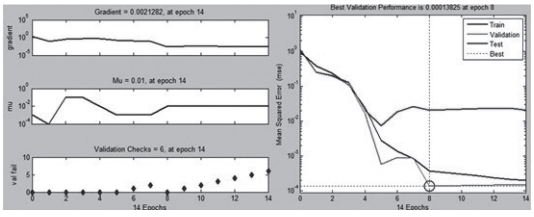


Рис. 3. Обучение нейронной сети

Результат работы нейронной сети: 1.0447, 1.0375, 1.0072, 2.0398, 2.1344, 1.8649 ; 2.9377 , 2.9987, 2.9965. Неточность в определении пользователя можно списать на недостаточный выбор метрики нейронной сети с прямым распространением сигнала и обратным распространением ошибки и, как следствие, неправильное вычисление весовых коэффициентов.

Иерархическая сеть**.** Минимальное количество повторений парольной фразы при которой удалось добиться корректной процедуры распознавания зарегистрированного пользователя составило 5 раз. В ходе выполнения данного алгоритма на каждом шаге объединяются два кластера с наименьшим расстоянием между двумя другими кластерами. Максимальное количество пользователей при котором возможна корректная аутентификация, вследствие подчинённости иерархии, составило 50 человек.

Самоорганизующаяся карта Кохонена. В ходе проведения эксперимента было зарегистрировано 3 пользователя. Минимальное количество повторений, при котором пользователь должен вводить ключевое слово составило 10 раз. При меньшем повторе парольной фразы наблюдались ошибки второго рода. При обучении нейронной сети обязательным условием следует указать общее количество выходов, которое равно количеству зарегистрированных пользователей. На рисунке видно, что образовалось 3 кластера. Временные интервалы между нажатиями клавиш с помощью весовых коэффициентов сгруппировались вокруг зарегистрированных пользователей.

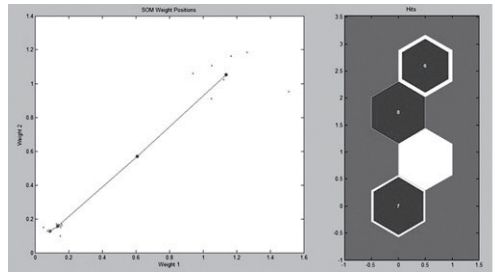


Рис. 4. Кластерное распознавание пользователей

На рисунке ниже представлен процесс обучения самоорганизующейся карты Кохонена, порядок ошибки которой составил 7×10^{-1}, что не удовлетворяет заданным требованиям эффективности биометрической системы.

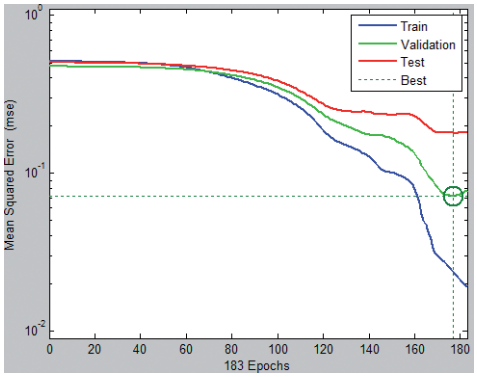


Рис. 5. График зависимости среднеквадратической ошибки от итераций обучения

На графике зависимости среднеквадратической ошибки от итераций обучения показаны оценки ошибки для трёх наборов данных: тренировочного, валидационного и тестового. При этом обучение прекращается, когда ошибка в валидационном наборе данных перестаёт уменьшаться. Тестовый набор представлен на графике сплошной линией, который показывает обобщающую способность сети.

Основным применением данной сети является скрытый мониторинг компьютерных информационных систем безопасности.

Нейронная сеть, у которой количество входов равняется количеству выходов. Минимальное количество повторений парольной фразы при которой удалось добиться корректной процедуры распознавания зарегистрированного пользователя составило 8 раз. Каждому пользователю отведён свой выходной слой. Это позволяет исключить ошибки второго рода. Из каждого набора входных слоёв выбирает ровно один вектор, который и характеризует данный слой. На рисунке ниже представлен график кривой ошибки. Площадь под кривой составила 0,846. Чем ближе данное значение к 1, тем лучше модель классификации обучена. Точность распознавания высчитывается как количество правильно распознанных пользователей к общему числу зарегистрированных пользователей и в данном случае равно 0,746.

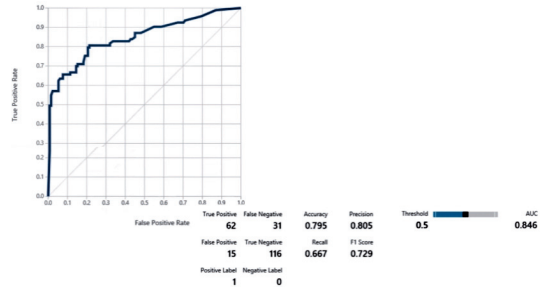


Рис. 6. Процесс обучения

Исходя из вышеперечисленного была выбрана нейронная сеть, которая оптимальным образом подходит для проведения аутентификации по клавиатурному почерку – нейронная сеть, у которой количество входов равняется количеству выходов. Она обладает достаточной устойчивостью и оптимально распознаёт зарегистрированных пользователей. Большим плюсом является большое количество пользователей при которой возможна корректная аутентификация. Существенным недостатком иерархической сети является малое количество пользователей, которое может обрабатывать данная сеть. Использование нейронной сети Кохонена возможно в качестве вторичной аутентификации, так как данная сеть не всегда способна отделить входные данные зарегистрированного пользователя от нелегитимного. Данная сеть хорошо показывает сам процесс кластеризации. Нейронная сеть с прямым распространением сигнала устойчиво распознает пользователей, но их количество, которая она может обработать, существенно ограничено.

Статья выполнена при поддержке Правительства РФ (Постановление №211 от 16.03.2013 г.), соглашение № 02.A03.21.0011.

Литература

1. Осовский С. Нейронные сети для обработки информации / пер. с польского И. Д. Рудинского. – М. : Финансы и статистика, 2002. – 344 с.

2. Асяев Г. Д., Рагозин А. Н. Определение минимального набора входных данных для корректной аутентификации по клавиатурному почерку с использованием нейронной сети // Вестник УрФО. Безопасность в информационной сфере. – 2017. – № 3(25).

References

1. Osovskiy S., Neural networks for information processing / Trans. from the Polish I.D.Rudinsky .- Moscow: Finance and Statistics, 2002. – P. 344.

2. Asyaev G.D, Ragozin A.N. Determination of the minimum set of input data for correct authentication using keypad handwriting using a neural network // Vestnik URFO. Security in the information sphere. – Chelyabinsk: Izd. Center SUSU, 2017. – № 3 (25).

АСЯЕВ Григорий Дмитриевич, студент высшей школы электроники и компьютерных наук кафедры «Защита информации» Южно-Уральского государственного университета. Россия, 454080, г. Челябинск, пр. Ленина, д. 76. E-mail: asyaev1996@mail.ru

РАГОЗИН Андрей Николаевич, кандидат технических наук, доцент кафедры «Защита информации», доцент кафедры «Инфокоммуникационных технологий» ФГАОУ ВО «Южно-Уральский государственный университет» (Национальный исследовательский университет). Россия, 454080, г. Челябинск, пр. Ленина, д. 76. E-mail: asyaev1996@mail.ru

ASYAEV Grigoriy, Higher School of Electronics and Computer student of the Department of Science "Information security" of the South Ural State University. Russia, 454080, Chelyabinsk, Lenin Avenue, 76. E-mail: asyaev1996@mail.ru

RAGOZIN Andrey, Ph.D., Candidate of Technical Sciences, assistant professor of information security , assistant professor of information and communication technologies FGAOU «South Ural State University» (National Research University). Russia, 454080, Chelyabinsk, Prospekt Lenina, 76. E-mail: asyaev1996@mail.ru

УДК 004.048 Вестник УрФО № 1(27) / 2018, с. 9–13

Швырев Б. А., Бердник М. В.

ИССЛЕДОВАНИЕ ПАССИВНОЙ РАДИОЗАКЛАДКИ С ФАЗОВОЙ МОДУЛЯЦИЕЙ ПЕРЕИЗЛУЧЁННОГО ПОЛЯ

Рассматривается работа пассивной радиозакладки с фазовой модуляцией переизлученного сигнала. Проведены экспериментальные измерения передачи сигнала. Полученные результаты свидетельствуют о реализуемости акустического канала утечки информации по средствам пассивной радиозакладки с фазовой модуляцией переизлучённого поля

Ключевые слова: *пассивная радиозакладка, акустический канал утечки, фазовая модуляция.*

Shvyrev B. A., Berdnik M. V.

INVESTIGATION OF A PASSIVE RADIO BOOKMARK WITH PHASE MODULATION OF THE RERADIATED FIELD

The work of a passive radio pad with phase modulation of the re-emitted signal is considered. Experimental measurements of signal transmission are carried out. The obtained results testify to the feasibility of an acoustic channel for information leakage through passive radiolocating means with phase modulation of the reradiated field

Keywords: *passive radio coverage, acoustic leak channel, phase modulation.*

Эффективным способом защиты от утечки по акустическому каналу является обнаружение радиозакладных устройств внутри защищаемого помещения. Стремительное развитие беспроводных технологий и микроэлектронной базы приводит к возобновлению интереса к пассивным радиозакладкам.

Рассмотрим работу пассивной переизлучающей радиозакладки. При протекании информационного низкочастотного тока через полупроводниковый диод, установленный в разрыв полуволнового диполя, в прямом направлении выводы диода четвертьволновые вибраторы соединяются, образуя единый полуволновый вибратор с резонансным распределением тока и большим значением эффективной поверхности рассеивания (ЭПР), чем два четвертьволновых вибратора, при протекании тока в обратном направлении. Перепад значений ЭПР во время действия информаци-

онного сигнала приводит к амплитудной модуляции переотраженного сигнала [1].

Одна из основных характеристик акустического канала утечки акустической информации с использованием переизлучающей радиозакладки это дальность обнаружения сигнала переотраженного радиозакладкой на фоне сигналов отражённых другими объектами. Дальность обнаружения зависит от рабочих характеристик приёмника, которые представляют собой вероятность правильного обнаружения при заданной вероятности ложной тревоги. Известно, что в зависимости от вида модуляции меняются и рабочие характеристики оптимального приёмника [3].

Для реализации радиозакладок наиболее часто используется амплитудная модуляция переизлучённого сигнала. В литературе [1; 2] приводится величина порядка 10 % для глубина амплитудной модуляции от максимально возможного переизлученного сигнала. Для повышения вероятности обнаружения в условиях высоких фоновых отражений целесообразно использовать не только амплитудную, но и фазовую модуляцию перизлучённого поля.

Максимальная точность обнаружения определяется скоростью приращения фазы переизлученного радиозакладкой сигнала определяемая противофазным сложением сигналов переизлученных составляющими радиозакладку элементарных диполей, при этом отношение сигнал/шум стремится к нулю. Так при одинаковом энергетическом отношении сигнал-шум вероятность правильного обнаружения у сигналов с фазовой модуляцией выше, чем у сигналов с амплитудной модуляцией [3].

Для улучшения рабочих характеристик приёмника исследуем работу радиозакладки, созданной на основе системы диодов включенных в полуволновый вибратор – параметрический фазовый модулятор. Схема параметрического фазового модулятора и экспериментальной установки приведена на рис. 1.

Фазовый модулятор состоит из двух пассивных переизлучателей с амплитудной модуляцией расположенных на расстоянии в четверть длины волны друг от друга, которые управляются генератором низкой частоты ГНЧ через ключи $К_1$ и $К_2$. ГНЧ выбран в качестве модели информационного источника акустической информации. Экспериментальная установка состоит из высокочастотного генератора ГВЧ, излучающей антенны С, двух направленных ответвителей, аттенюатора А и фазовращателя Ф, расположенных в канале опорной волны, диода Д с фильтром Ф1, селективного вольтметра В.

Опишем прохождение сигнала через экспериментальную установку. Сигнал на входе диода равен

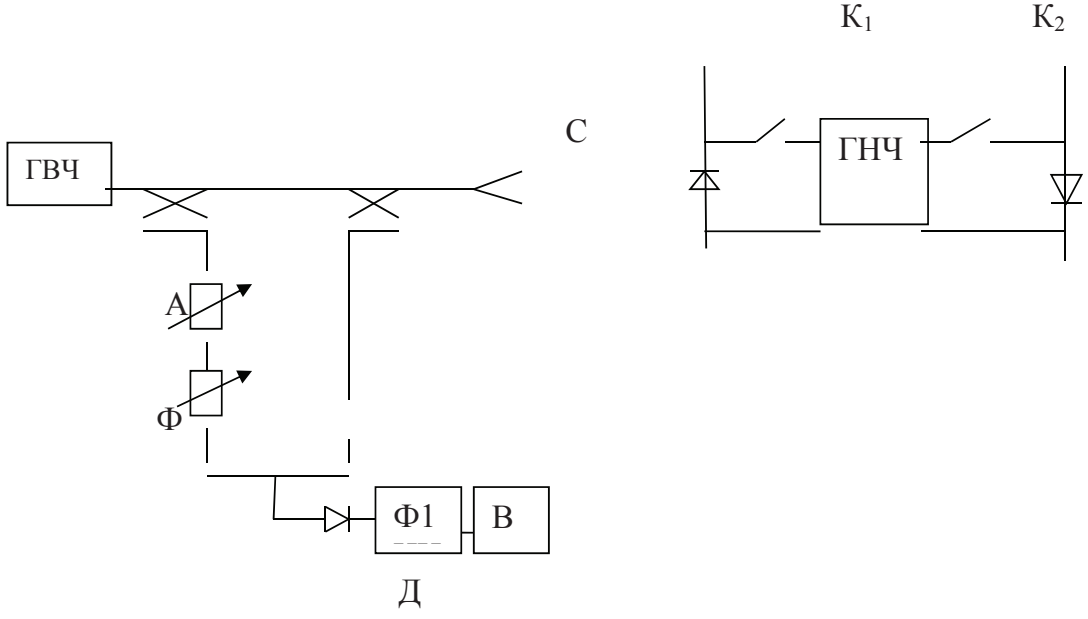


Рис. 1. Схема экспериментальной установки

$$u(t) = U_0 \cos(\omega_0 t + \varphi_0) + \\ + U(t) \cos(\omega_0 t + \varphi_1), \quad (1)$$

где U_0 ,φ_0 – фонового опорного сигнала,

U(t) = U(1 + McosΩt) – закон амплитудной модуляции сигнала переотраженного радиозакладкой при замыкании ключей K_1 или K_2,

M – глубина модуляции сигнала,

Ω – частота модуляции, задаваемая генератором ГНЧ.

Выберем суммарную амплитуду сигнала за счет регулировок сигнала в канале опорной волны так, чтобы вольт-амперную характеристику диода можно было бы считать квадратичной $i = \alpha u^2$, тогда ток на выходе диода равен

$$i(t) = \alpha[U_0 \cos(\omega_0 t + \varphi_0) + \\ + U(t) \cos(\omega_0 t + \varphi_1)\,]^2 = \\ б\{U_0^2/2 + U_0^2/2 \cos[2(\omega_0 t + \varphi_0)] + \\ t + \varphi_0)] + U^2(t)/2 + U^2(t)/ \\ /2 \cos[2(\omega_0 t + \varphi_1)] + \\ U_0 U(t) \cos(\varphi_1 - \varphi_0) + \\ + U_0 U(t) \cos(2\omega_0 t + \varphi_0 + \varphi_1)\}. \quad (2)$$

Напряжение на выходе низкочастотного фильтра детектора имеет вид

$$u_1(t) = z_1(i\omega) i(t) = \alpha R[U_0^2/2 + \\ + U^2(t)/2 + U_0 U(t) \cos(\varphi_1 - \varphi_0)'] \quad (3)$$

где $z_1(i\omega)$ – частотная характеристика фильтра,

R – его сопротивление в области нижних частот.

Раскрывая значение функции U(t) получим

$$u(t) = \alpha R\{U_0^2/2 + U^2(1 + M^2/2)/2 + \\ + U_0 U \cos(\varphi_1 - \varphi_0) + UM[U + \\ + U_0 \cos(\varphi_1 - \varphi_0)] \cos \Omega t + U^2 M^2/4 \cos 2\Omega t\}. \quad (4)$$

Обычно, $U_0 \gg U$ поэтому для выделения второй гармоники уменьшим расстояние между рассеивателем и приёмно-передающей антенной на столько, чтобы уверенно наблюдать вторую гармонику на выходе селективного вольтметра. Для обеспечения контроля квадратичности вольт-амперной характеристики диода регистрировалось значение амплитуды третьей гармоники, которая, при её квадратичности, равняется нулю. Если амплитуда третьей гармоники не равна нулю, то суммарная амплитуда сигнала, поступающего на диод может быть уменьшена с помощью регулировок в канале опорной волны до значений, при котором амплитуда третьей гармоники уменьшится до нуля.

В случае если замкнуты оба ключа K_1 и K_2, сдвиг фазы переотраженного сигнала от антенн становится *πn* каждый момент времени, тогда присутствует отражение от полуволнового вибратора, роль которого выполняет первый или второй вибратор в зависимости от приложенного напряжения и амплитудная модуляция сигнала не происходит. Однако, из-за несовпадения ЭПР вибраторов в полуволновом и четвертьволновом режимах, а также из-за различия их положения как директора и рефлектора в двухэлементной антенне в суммарном сигнале присутствует паразитная амплитудная модуляция с глубиной M_1.

Разность фаз $\varphi_1 - \varphi_0$ будет меняться. Если отражение идет от первого полуволнового вибратора по отношению к приёмной антенне, то разность фаз $\varphi_1 - \varphi_0 = 0$, если второй то $\varphi_1 - \varphi_0 = \pi$. Это означает, что на диод поступает фазоманипулированный сигнал. Аппроксимируем изменение фазы $\varphi_1 - \varphi_0 = m\sin\Omega t$, где m – индекс модуляции, зависящий от расстояния между диодами-диполями. Тогда сигнал на выходе низкочастотного фильтра детектора имеет вид:

$$u_2(t) = \alpha R\{U_0^2/2 + U^2(1 + M_1^2/2)/2 + \\ + U_0 U \sum_{k=-\infty}^{k=\infty} J_0(m) \cos k\Omega t + \\ + UM_1[U + U_0 \cos \Omega t \sum_{k=-\infty}^{k=\infty} J_0(m) \cos k\Omega t] + \\ + U^2 M_1^2/4 \cos 2\Omega t\} \quad (5)$$

Из полученного соотношения видно, что в спектре сигнала $u_2(t)$ появились новые гармоники с амплитудой пропорциональной $J_0(m)$, где $J_0(m)$ – функция Бесселя к-го порядка. Известно, что при $k < m + 1$ в спектре сигнала амплитуды гармоник отличны от нуля. При m = 3,14 третья гармоника спектра отлична от нуля и её обнаружение будет свидетельствовать об обогащении спектра сигнала в целом. Заметим, что отсутствии паразитной амплитудной модуляции $M_1 = 0$ и $u_2(t)$ равно

$$u_2(t) = \alpha R\{U_0^2/2 + U^2/2 + \\ + U_0 U \sum_{k=-\infty}^{k=\infty} J_0(m)\cos k\Omega t\}, \quad (6)$$

И для обнаружения обогащения спектра достаточно было бы зафиксировать наличие первой или второй гармоники.

Экспериментальное определение наличия третьей гармоники на выходе селективного вольтметра было выполнено при выполнении контроля за квадратичностью вольтамперной характеристики диода по выше приведенной методике. В качестве диодов, управляющих полуволновым вибратором использовались полупроводниковые диода типа 1N4148, частота модуляции $\Omega/2\pi$ = 1200 Гц. На выходе селективного вольтметра наблюдался сигнал с амплитудным отношением сигнал-шум 9. При размыкании одного из переключателей $К_1$ или $К_2$ амплитуда сигнала на третьей гармонике уменьшалась до уровня шума.

Полученные результаты свидельствуют о том, что важная характеристика управляемого пассивного рассеивателя может быть увеличена путем применения двух диодов-диполей расположенных последовательно и, через которые поочередно проходит ток от источника информационного сообщения.

Реализация рассмотренной пассивной радиозакладки в целом усложняет конструкцию переизлучателя, требует наличие элемента коммутации отражателями которым может выступать генератор низкой частоты, что можно рассматривать как демаскирующее свойство. Наличие генератора требует наличие источника питания или мощного облучающего сигнала. Возможность реализации фазомодулированного переотраженного сигнала позволяет использовать все свойства такой модуляции – улучшенное энергетическое соотношение в условиях больших фоновых переотражений, и соответственно дальность передачи информации, что увеличивает территорию, из которой может быть совершен несанкционированный съем акустической информации. Полученные результаты позволят совершенствовать рекомендации по предотвращению утечки информации по рассмотренному каналу.

Литература

1. Струков И. Ф. Оперативный анализ пространственных характеристик электромагнитных полей с помощью управляемых рассеивателей : дис. канд. физ.-мат. наук. – Воронеж, 1983.

2. Нелинейная радиолокация : сб. ст. / под ред. А. А.Горбачёва, А. П. Колданова, А. А. Потапова, Е. В. Чигина. – Ч. 1 – М. : Радиотехника, 2005.

3. В. И. Тихонов Оптимальный прём сигналов. – М. : Радио и связь,1983.

Reference

1. Strukov I. F. Operativnyj analiz prostranstvennyh harakteristik jelektromagnitnyh polej s pomoshh'ju upravljaemyh rasseivatelej. Dis. kand. fiz.-mat. nauk. – Voronezh, 1983.

2. Nelinejnaja radiolokacija. Sbornik statej. Chast' 1 / Pod red. A. A. Gorbachjova, A. P. Koldanova, A. A. Potapova, E. V. Chigina. – M. : Radiotehnika, 2005.

3. V. I. Tihonov Optimal'nyj prjom signalov. – M.: Radio i svjaz', 1983.

ШВЫРЕВ Борис Анатольевич, кандидат физико-математических наук, доцент кафедры компьютерных технологий и информационной безопасности. Кубанский государственный технологический университет. 350000 г. Краснодар, ул. Московская, 2. E-mail: bor2275@yandex.ru

БЕРДНИК Мария Викторовна, доцент кафедры компьютерных технологий и информационной безопасности. Кубанский государственный технологический университет. 350000 г. Краснодар, ул. Московская,2. E-mail: marviktr@mail.ru

SHVYREV Boris, Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Computer Technologies and Information Security. Kuban State Technological University. 350000, Krasnodar, Bld. 2 Moskovskaya street. E-mail: bor2275@yandex.ru

BERDNIK Maria, Associate Professor of the Department of Computer Technologies and Information Security. Kuban State Technological University. 350000, Krasnodar, Bld. 2 Moskovskaya street. E-mail: marviktr@mail.ru

УДК 004.056.53 Вестник УрФО № 1(27) / 2018, с. 14–18

Баранкова И. И., Михайлова У. В., Лукьянов Г. И.

РАЗРАБОТКА СИСТЕМЫ WORDSEARCH ДЛЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ

Конфиденциальность информации организации или предприятия является важной составляющей, и нарушение ее может нанести значительный ущерб. На сегодняшний день существует большое количество способов и методов борьбы с утечками конфиденциальной информации. Одним из возможных и наиболее эффективных способов защиты информации это внедрение системы защиты от утечек конфиденциальных данных Data Leak Prevention (DLP). В статье приведены этапы разработки программы и результаты анализа информационного потока в корпоративной сети. Произведена оценка работы поисковых алгоритмов подстроки в строках на качественные и временные показатели. Благодаря сравнительному анализу определены слабые стороны используемых алгоритмов, а так выявлены способы обхода системы поиска. Разработаны методика использования базы конфиденциальных данных и алгоритм подстрочного поиска в электронных документах. Внедрение методики обработки базы искомых данных перед запуском поточного сканирования значительно повысило качественную характеристику системы поиска и при этом незначительно увеличило время выявления инцидентов. Произведена модернизация модуля агента с целью блокировки дальнейших манипуляций с информацией и персональной машиной при обнаружении инцидентов. Благодаря данным доработкам получилось значительно повысить эффективность разработанной системы, а именно снизить уровень утечки конфиденциальной информации.

Ключевые слова: *корпоративна сеть, конфиденциальная информация, утечка информации, DLP система, поиск подстрок в строке, WordSearch, блокировка персональной машины.*

DEVELOPMENT OF THE WORDSEARCH SYSTEM TO PROTECT FROM CONFIDENTIAL INFORMATION LEAKAGE

Confidentiality of information of the organization or the enterprise is an important component, and its violation can cause considerable damage. To date, there are a large number of ways and methods to combat the leakage of confidential information. One of the possible and most effective ways to protect information is the introduction of a system to protect against data leak Prevention (DLP). The article presents the stages of the program development and the results of the analysis of the information flow in the corporate network. The work of search algorithms of substring in lines on qualitative and temporal indexes is estimated. Due to the comparative analysis the weaknesses of the used algorithms are determined, as well as the ways to bypass the search system are revealed. The method of using the confidential data base and the algorithm of string search in electronic documents are developed. The introduction of the technique of processing the database of the required data before the launch of line scanning significantly improved the quality of the search system and thus slightly increased the time of incident detection. Upgrading module agent to block further manipulation of the information and personal machine upon detection of incidents. Thanks to these improvements it was possible to significantly improve the efficiency of the developed system, namely to reduce the level of leakage of confidential information.

Keywords: *corporate network, confidential information, information leak, DLP system, search for substrings in the string, WordSearch, lock the personal machine.*

В настоящее время один из возможных и наиболее эффективных способов мониторинга информационного потока предприятия и методов борьбы с действиями злоумышлиников являются системы защиты от утечек конфиденциальных данных Data Leak Prevention [1; 2]. Под DLP системой понимают технологии предотвращения утечек конфиденциальной информации из информационной системы, а также программные или программно-аппаратные комплексы для предотвращения различных видов утечек информации [3; 4].

Обнаружение и блокировка передачи информации из корпоративной системы в сеть осуществляется путем применения ряда стандартных функций, а именно:

– фильтрация интернет-трафика, иных информационных потоков;

– анализ контента по предварительно установленным ключевым словам, определенным выражениям, «оцифрованным» документам, учитывая совокупность всех обстоятельств [5].

Разработка системы WordSearch

Обнаружение конфиденциальной информации в DLP системах реализуется за счет применения совокупности методов поиска слов и словосочетаний по словарю и синтаксического разбора текстовых строк по формализованному шаблону (WordSeach).

Основные алгоритмы WordSeach используемые во многих DLPсистемах:

1) линейный поиск;

2) поиск Д. Кнута, Д. Мориса и В. Пратта (КМП – поиск);

3) Поиск Р. Бойера и Д. Мура (БМ-поиск);

4) Нечеткий поиск в тексте.

На основе первых трех, приведенных выше, алгоритмов поиска разработано приложение, которое производит поиск подстроки в представленном тексте (рис. 1). С использованием данного приложения про-

изведен сравнительный анализ алгоритмов поиска.

При реализации простого поиска (брут) были осуществлены доработки использования базы.

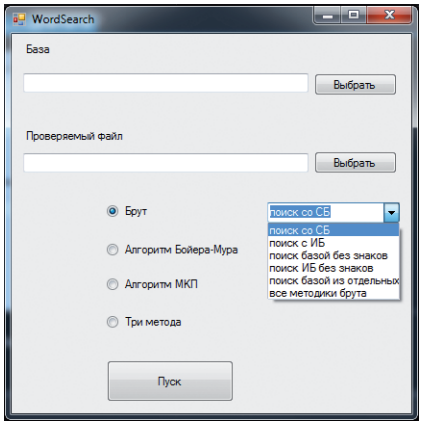


Рис. 1. Стартовое окно разработанного приложения для поиска подстроки в тексте

В результате тестирования каждого метода все они показали достаточно высокие результаты поиска. Из-за отсутствия разнородной интерпретации базы искомой информации методы КМП и БМ показали результаты ниже чем у метода «Брута». После доработки КМП и БМ методов, произведена оценка временного показателя каждого алгоритма. В качестве тестового текста использовали текст длинной 10002 символа. Характеристики стенда, на котором проводилось тестирование: CPUAthlonx4 640, ОЗУ 4Gb, Windows 10(32-bit) Pro. Результаты тестирования представлены в виде таблицы.

После доработки методов алгоритм Бойера – Мура показал наилучшее время выполнения поставленной задачи поиска.

Время работы алгоритмов поиска при различной длине искомой подстроки

Алгоритм	Время выполнения(мс)		
	Длина ≤ 10	Длина ≤ 100	Длина ≤ 250
Брут	15	93	234
КМП	5	30	50
БМ	31	31	32

Производительность всех исследуемых алгоритмов поиска представлена в графическом виде на рис. 2.

В связи с множественными поправками по базе искомых строк из-за искажения исследуемого текста, такого как замена букв,

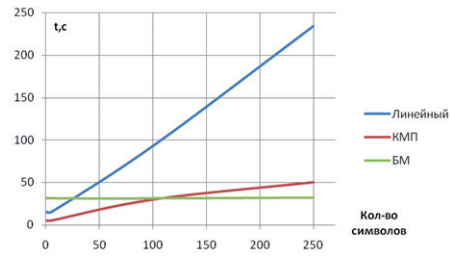


Рис. 2. Производительность алгоритмов поиска

перестановка и разрыв слов и т. п., наиболее эффективным и быстродействующий методом показал себя метод нечеткого поиска. Алгоритмы нечеткого поиска применяются в текстовых редакторах для проверки орфографии и во всем известных поисковых системах. Примером работы такой функции является вывод сообщения пользователю при запросе в поисковой системе «Возможно, вы имели ввиду…». Но как и остальные алгоритмы этот алгоритм можно обойти, поэтому необходима доработка модулей обработки сканирования перед полным внедрение алгоритма нечеткого поиска в систему.

В разработанном приложении реализована блокировка персонального компьютера сотрудника в случае обнаружения совпадений. При обнаружении искомых файлов будет произведено отключение сетевых подключений, а так же блокировка мышки и клавиатуры. При этом на экране вызовется окно с предупреждением о найденных совпадениях (рис. 3).

Рис. 3. Уведомление о найденных совпадениях

Данная блокировка снимается персоналом ответственным за работу данного ПО (сотрудники отдела безопасности). Для снятия блокировки необходимо указать в программе, какой комбинацией клавиш она будет производиться.

Заключение

С использованием разработанного нами приложения произведена оценка работы ал-

горитмов поиска подстрок в строке. При этом выявлено, что зная алгоритм каждого метода, злоумышленник может обойти DLP-систему. В результате проведенного анализа сделаны следующие выводы:

1. Необходимы разработка и создание нового алгоритма поиска с оптимальной скоростью работы, а так же учетом недостатков уже известных алгоритмов.

2. DLP система не является достаточной защитой от утечки информации, поэтому необходимо использование комплекса систем и организационных мер.

Литература

1. Баранкова И. И., Михайлова У. В., Лукьянов Г. И. DLP система: защита от утечки информации. Анализ поиска WordSearch // Актуальные проблемы современной науки, техники и образования. – 2016. – Т. 1. – № 1. С. 187–191.

2. Баранкова И. И., Михайлова У. В., Лукьянов Г. И. Прогнозирование локальных и внешних угроз на информационные серверы предприятия // Актуальные проблемы современной науки, техники и образования. – 2017. – Т. 1. – С. 217–220.

3. Баранкова И. И., Михайлова У. В., Самохвал В. Д., Огонесян Ш. У. Анализ информационных угроз ВУЗА // Актуальные проблемы современной науки, техники и образования. – 2013. – Т. 2. – № 71. – С. 157–159.

4. Коновалов М. В., Михайлова У. В., Хусаинов А. А., Санарбаев Р. Ж. Алгоритмы шифрования данных // Актуальные проблемы современной науки, техники и образования. – 2013. – Т. 2. – № 71. – С. 159–161.

5. Михайлова У. В., Коновалов М. В., Гуринец К., Кучербаева Э. Ф. Идентификация личности // Актуальные проблемы современной науки, техники и образования. – 2013. – Т. 2. – № 71. – С. 164–166.

References

1. Barankova I.I, Mikhailova U.V., Lukyanov G.I. DLP sistema: zashchita ot utechki informatsii. Analiz poiska WordSearch[DLP system: protection against information leakage. WordSearch search analysis] // Aktual'nye problemy sovremennoy nauki, tekhniki i obrazovaniya [Actual Problems of Modern Science, Technology and Education], 2016. T. 1. № 1. P. 187-191.

2. Barankova I.I, Mikhailova U.V., Lukyanov G.I. Prognozirovanie lokal'nykh i vneshnikh ugroz na informatsionnye servery predpriyatiya [Forecasting of local and external threats to enterprise information servers] // Aktual'nye problemy sovremennoy nauki, tekhniki i obrazovaniya [Actual Problems of Modern Science, Technology and Education], 2017. T. 1. P. 217-220.

3. Barankova I.I, Mikhailova U.V., Samohval V.D., Oganesyan Sh.U. Analiz informatsionnykh ugroz VUZA [Analysis of information threats of the University] // Aktual'nye problemy sovremennoy nauki, tekhniki i obrazovaniya [Actual Problems of Modern Science, Technology and Education], 2013. T. 2. № 71 P. 157-159.

4. Konovalov M.V., Mikhailova U.V., Husainov A.A., Sanarbaev R.J. Algoritmy shifrovaniya dannykh [Data Encryption Algorithms] // Aktual'nye problemy sovremennoy nauki, tekhniki i obrazovaniya [Actual Problems of Modern Science, Technology and Education], 2013. T. 2. № 71 P. 159-161.

5. Mikhailova U.V., Konovalov M.V., Gurinec K., Kucherbaeva E.F. Identifikatsiya lichnosti [Identification of a person] // Aktual'nye problemy sovremennoy nauki, tekhniki i obrazovaniya [Actual Problems of Modern Science, Technology and Education], 2013. T. 2. № 71 P. 164-166.

БАРАНКОВА Инна Ильинична, доктор технических наук, заведующий кафедрой ИиИБ, Магнитогорский государственный технический университет им. Г. И. Носова. 455000, г. Магнитогорск, пр. Ленина 38. E-mail: inna_barankova@mail.ru

МИХАЙЛОВА Ульяна Владимировна, кандидат технических наук, доцент кафедры ИиИБ, Магнитогорский государственный технический университет им. Г. И. Носова. 455000, г. Магнитогорск, пр. Ленина 38. E-mail: ylianapost@gmail.com

ЛУКЬЯНОВ Георгий Игоревич, ассистент кафедры ИиИБ Магнитогорский государственный технический университет им. Г.И. Носова 455000, г. Магнитогорск, пр. Ленина 38. E-mail: decorsi@mail.ru.

BARANKOVA Inna, Department, Nosov Magnitogorsk State Technical University (NMSTU), D.Sc.,Head of Computer Science and Information Safety Engineering (CSISE), Bld. 38, Lenina Ave, Magnitogorsk, Russia, 455000. E-mail: inna_barankova@mail.ru;

MIKHAILOVA Uliana, NMSTU, Ph.D.,Associate Professor of CSISE Department, Bld. 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: ylianapost@gmail.com;

LUKIANOV Georgy, NMSTU, Teaching Assistant of CSISE Department, Bld. 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: decorsi@mail.ru.

УДК 004.048 Вестник УрФО № 1(27) / 2018, с. 19–23

Власенко А. В., Бердник М. В., Швырев Б. А.

ИССЛЕДОВАНИЕ ПРОГРАММНЫХ РЕШЕНИЙ РЕГИСТРАЦИИ И ЗАПИСИ СОБЫТИЙ КЛАВИАТУРЫ

В данной статье рассматривается вопрос идентификации пользователя по его уникальному клавиатурному подчерку. В частности, рассматриваются различные механизмы идентификации, такие как скорость письма, сила нажатия на клавиши и другие способы. Представлен алгоритм процесса регистрации времени нажатия и отпускания клавиши. Изложены основные методы регистрации состояния клавиш.

Ключевые слова*: клавиатурный почерк, идентификация, события клавиатуры, методы регистрации.*

Vlasenko A. V., Berdnik M. V., Shvyrev B. A.

RESEARCH OF SOFTWARE SOLUTIONS FOR REGISTRATION AND RECORDING OF KEYBOARD EVENTS

This article discusses the problem of identifying a user using a unique key combination. In particular, various identification mechanisms are considered, such as letter speed, keystrokes and other methods. The algorithm of the process of recording the time of pressing and releasing the key is presented. The main methods for registering the state of keys are described.

Keywords: *keyboard handwriting, identification, keyboard events, registration methods.*

Использование интернет-мессенджеров в личной и деловой переписке является реалиями сегодняшней жизни. Не смотря на все плюсы информационного обмена в виртуальной среде, одной из основных проблем является идентификация пользователя, находящегося по ту сторону экрана. На сегодняшний момент существует достаточно много технологий позволяющих как определить, так и обойти получение информации о месте нахождения, конечном адресе устройства, с которого передается информация.

Наиболее интересным направлением, с нашей точки зрения, в области идентификации пользователя, является анализ клавиатурного почерка. Важность и точность этого метода в нецифровой среде подтверждена наличием такой науки как графология, суще-

ствованием графологической экспертизы, исследований, связанных с определением по почерку образа жизни, пола, возраста, профессии человека.

Большинство исследований в области анализа клавиатурного почерка были связаны с оценкой особенности работы профессиональных наборщиков текста. Сейчас, когда социальные сети становятся достаточно существенным инструментом, в том числе и информационного противоборства, важно разработать механизм, позволяющий идентифицировать лицо, отправляющее короткие сообщения (размером до 300 знаков).

Одним из достоинств идентификации пользователя по клавиатурному подчерку является использование стандартной клавиатуры, подключенной к персональной ЭВМ стандартным интерфейсом PS\2 или USB. Устройства регистрации биометрических данных пользователей обладают высокой стоимость ограничивающей их применимость в системах безопасности. К тому же эти устройства используют специальные интерфейсы и контроллеры для передачи данных в компьютер, использование которых сопряжено с трудностями установки, настройки и калибровки, а также ограничивает мобильность устройства идентификации. Клавиатура как устройство биометрической идентификации лишено этих недостатков. Для ввода информации не требуется дополнительных аппаратных преобразователей.

С целью повышения информативности биометрической информации пользователя предложено использовать дополнительный контроллер, отслеживающий параметры надавливания клавиши. При надавливании происходит изменение расстояния между контактами электрической группы конечной площади. Контактная пара рассматривается как параметрическая емкость, изменяемая при нажатии на клавишу. Скорость изменения емкости клавиш при нажатии имеет индивидуальную составляющую. Мы предлагаем использовать этот параметр для повышения достоверности идентификации пользователей.

Целесообразность использования предложенного устройства вызвана тем, что контроллер стандартной клавиатуры выполняет функцию компаратора и обрезает временную форму длительности импульса нажатия клавиши. Для борьбы с дребезгом контактов и снижения ошибок интерпретации контроллер вводит временную задержку.

Создание дополнительного контроллера приведет к увеличению стоимости устройства, что может негативно сказать на востребованности метода.

Анализ источников показал, что большинство исследований клавиатурного подчерка посвящено изучению индивидуальных особенностей пользователей на основе интервалов времени между нажатиями клавиш и длительности удержания клавиш. По измеренным значениям интервалов находились производные характеристики, такие как скорость нажатия одной или группы клавиш, среднее значение интервала между нажатиями, длительности перекрытий клавиш, длительность биграмм и триграмм и т. д. Исследователи в меньше степени уделяли внимание анализу длительности удержания клавиши и построению модели этого процесса, при этом рядом исследователей отмечается высокая информативность этих параметров для идентификации пользователей.

Все события клавиатуры, подключенной к компьютеру, регистрируются программными средствами. Процесс формирования массива экспериментальных данных связан с определением точности предполагаемых измерений. Для этого проанализируем исследуемый процесс набора текста на клавиатуре. Набор могут осуществлять две основные категории пользователей, обладающие навыком слепого набора или десятипальцевым способом и пользователи, печатающие одним пальцем. Считается что пользователь, обладающий десяти пальцевым набором текста, обладает большей вероятностью обнаружения, чем не имеющий такого навыка. Такие суждения справедливы в рамках распространенных моделей идентификации пользователей по средним значениям интервалов времени между нажатиями клавиш. Исходя из физиологических, анатомических и психических особенностей человека, мелкая моторика и динамика каждого индивида уникальна. Эти особенности обладают большим порядком малости, и для их описания и регистрации требуется использование максимально возможной точности измерения временных интервалов нажатия и отпускания клавиш. Скорость набора профессиональной машинистки составляет порядка 500–600 символов в минуту, в предположении последовательного набора символов интервал между нажатиями должен составлять 8,3 мс, без перекрытий, с минимальным физиологически объяснимым

временем удержания клавиши 50 мс. Для регистрации этих событий необходимо обеспечить регистрацию событий клавиатуры с интервалом порядка 4мс. Обычные пользователи, как и опытные наиболее вероятно нажимают клавиши с интервалом от 30 до 400 мс.

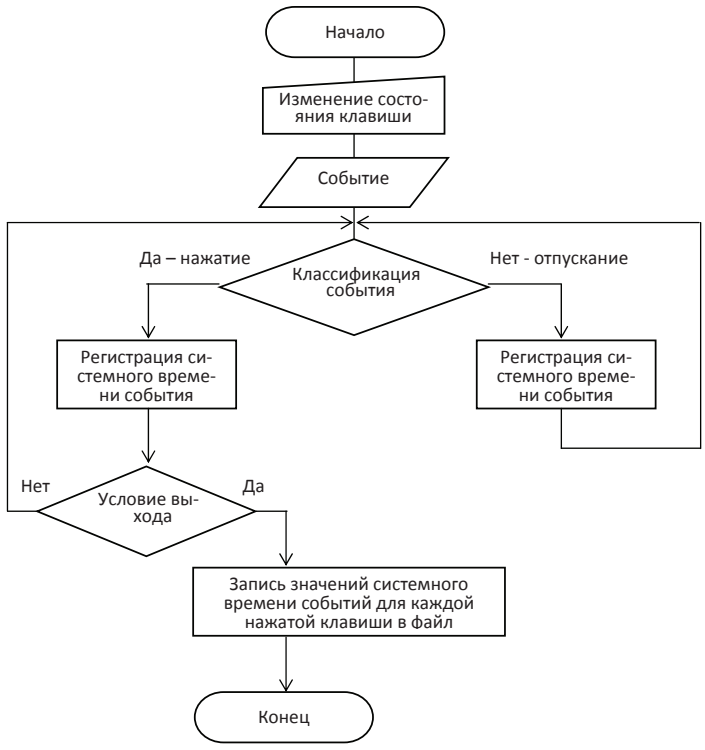
Рассмотрим программные решения для регистрации и записи событий клавиатуры, написанные на высокоуровневых языках программирования.

Клавиатура по своему назначению разрабатывалась как интерфейс с пользователем для ввода информации в компьютер с низкой скоростью. Это условие отразилось во всех языках программирования. От клавиатуры в стандартных и офисных программных продуктах не требуется высокая скорость передачи данных. Низкая скорость опроса клавиатуры компенсировалась наличием кольцевого буфера. Ситуация изменилась с развитием компьютерных игр, когда пользователь должен адекватно реагировать на очень динамичные изменения в виртуальном пространстве. Так игровая индустрия способствовала развитию программных средств DirectInput.

Методы регистрации временных характеристики ввода с клавиатуры, допускают реализации на разных языках программирования с вариантами внутренних алгоритмов и функций отсчета времени, фиксации измерений в файле. Для анализа возможности фиксации событий клавиатуры и оценки погрешности отсчетов разработаны три программы на разных языках высокоуровневого программирования реализующие основные методы сбора событий клавиатуры.

Общий алгоритм процесса регистрации времени нажатия и отпускания клавиши представлен на рисунке. Основные процессы алгоритма отследить нажатую клавишу, определить значение текущего времени и записать данные в файл. Алгоритм заключается в ожидании либо нажатия клавиши, либо её отпускания. При наступлении каждого из этих событий фиксируется системное время.

Для регистрации состояния клавиш используют три основных метода. Каждый метод использует обработку процессов на одном из трех основных этапах получения данных от клавиатуры приложением Windows. Каждый раз при нажатии на клавиатуру формируется событие Windows и передается запрашиваемому приложению, которое находится в фокусе. Для обслуживания клавиатуры в Windows существует специальный драйвер в виде файла динамической библиотеки с расширением dll. Он определяет скан код нажатой и отпущенной клавиши и преобразует его в ANSI код. Затем используется для форми-



Алгоритм сбора экспериментальных значений времени нажатия и отпускания клавиш

рования событий wm_keydown и wm_keyup, которые становятся в очередь событий для транспортировки их приложению в фокусе.

Основной способ регистрации, используемый большинством приложений, является обработка готовых сообщений Windows, таких как wm_keydown и wm_keyup находящихся в очереди событий. Для реализации такого приема написана программа на языке высоко уровня программирования C++. Она содержит обработку событий Windows и запись результатов в файл в формате txt.

Следующим подходом является использование setWinHook или программ перехвата событий Windows и минуя очередь событий запись в выходной файл. Для реализации такого приема написана программа на языке высоко уровня программирования Delphi 7.

Описанные выше приемы используют стандартный драйвер клавиатуры, предназначенный для своевременного нажатия клавиши обработки кольцевого буфера клавиатуры на случай невозможности своевременной обработки, а также отображения удержания служебных и специальных клавиш. Начиная с первых клавиатур персональных компьютеров драйвер, осуществлял регистрацию удержания клавиши, отсчет этого времени и запуск автоповтора скан кода соответствующей клавиши.

Большинство приложений современных операционных систем используют только время нажатия клавиши, время удержания не является информативным за исключением функции автоповтора символа на уровне операционной системы.

Время удержания клавиши так же является важным информационным параметром. Для исследования влияния временных характеристик отображения событий клавиатуры написана программа, реализующая функции драйвера. Для этого применены функции DirectInput из пакета Direct X 9.0. Разработанная программа на языке высоко уровня программирования C++ позволяла на прямую обращаться к устройству ввода клавиатуре и опрашивать её состояние с интервалов в единицы микросекунды. Работа программы использовала весь ресурс вычислительной машины, что приводило к «зависанию» компьютера. «Зависание» компьютера при выполнении этой программы наблюдалось на системах, обладающих самыми последними разработками бытовой вычислительной техники. Высокая точность регистрации отмечалась при полной передачи центральному процессору функции обработки событий клавиатуры. Уменьшение доли участия процессора в обработки состояния клавиатуры приводит к росту погрешности времени фиксации нажатия и времени удержания. Интервал дискретизации составляет порядка 15 625 мкс.

Анализ полученных результатов показал, что первый подход дает самую высокую погрешность регистрируемого времени удержания клавиши и составляет порядка 47 мс. Такое состояние объясняется использованием очереди событий Windows.

Использование Hook позволяет сократить погрешность до порядка 15 мс. Результат достигается за счет того, что при регистрации событий Windows программа минует очередь событий.

Все программные реализации обеспечили отличающиеся числовые значения между нажатиями клавиш и интервалов удержания для одной и той же контрольной группы пользователей. При этом отмечается схожесть частотной структуры распределения интервалов, удержания клавиш. Для каждого результата характерно увеличение числа интервалов удержания клавиши при наборе произвольного текста на кратных значениях.

Анализируемые программные решения использовали различные способы регистрации событий. Каждая программа имела некоторый интервал дискретизации по времени, или минимально регистрируемый интервал времени, эта величина в общем случае является погрешностью отображения. Программные особенности выполнения процедуры регистрации событий клавиатуры в полной мере не объясняют выявленные интервалы дискретизации. Задержки, сопутствующие этапам обработки событий и представления операционной системе имеют не постоянные значения порядка единиц мкс. Выявленная дискретизация отображения времени удержания клавиши от части определяется особенностью интерфейса соединения с компьютером. В п. 1.3 описывались возможные задержки во времени отображения, обусловленные интерфейсом передачи данных, но они носят системный характер и относятся ко всем передаваемым событиям. Одинаковая ошибка добавляется как к времени нажатия клавиши, так и ко времени ее отпускания.

Другой причиной дискретного отображения временных параметров является особенности регистрации текущего времени. Для определения времени нажатия клавиши необходи-

мо точно знать системное время или запускать дополнительный таймер, который также будет привязываться к системному времени.

Для синхронизации высокой точности на ОС Windows обычно использовался (Time Stamp Counter – счетчик отметок времени) TSC центрального процессора. Счетчик появился в x86 процессорах начиная с Pentium и является 64 разрядным. Он считывает тактовые импульсы центрального процессора. Значения счетчика TSC обычно запрашивается через инструкцию RDTSC пользователя. Эта операция легко и быстро выполняется и гарантирует высокую точность времени на современных компьютерах, порядка единиц микросекунд.

С развитием вычислительной техники и появления много ядерных систем, мобильных устройств частота процессора не остается постоянной в течение работы. Для экономии электроэнергии частота процессора мобильных вычислительных устройств уменьшается. При передачи задач между процессорами в многоядерной системе значение счетчика TSC изменяется и даже может показывать обратное время. TSC не всегда синхронизируется на двухядерных системах или SMP системах.

Для двухядерных систем Microsoft рекомендует использовать Query Performance Counter для синхронизации высокой точности порядка микросекунд. В двухядерной системе особенно при ее загрузке, TSC предоставляет программе использующей QPC значения частоты процессора не соответствующее текущему.

Вызов QueryPerformanceCounter и Time Get Tim приводит к изменению точности с микросекунд до миллисекунд, что более надежно. Большей надежностью и быстродействием, но низкой точностью обладает функция GetTickCount показавшая на Windows 9x минимальны интервал времени 55 мс.

Функция GetSystemTimeAdjustment возвращает значение приращения времени, возвращаемого GetTickCount. Как показали наблюдения (на компьютере с ОС Windows) эта функция возвращает 15625 мкс. Следовательно, GetTickCount возвращает время в миллисекундах, но с дискретностью в 15.625 мс. Системный таймер работает с этим периодом.

Проведенный анализ позволяет выделить ошибки в регистрации времени в самостоятельный класс погрешностей. Уменьшение величины ошибки приводит к нестабильности работы или «зависанию» вычислительной системы. Погрешность связана с архитектурными особенностями современных вычислительных систем. Для практических измерений выбирают компромисс между точностью и стабильностью работы вычислительной системы. Как показали измерения, дискретизация временных значений событий клавиатуры с интервалов ≈ 15 мс является оптимальным вариантом, при котором сохраняется работоспособность вычислительной системы.

ВЛАСЕНКО Александра Владимировна, доцент, кандидат технических наук, заведующий кафедрой компьютерных технологий и информационной безопасности Кубанский государственный технологический университет. 350000, г. Краснодар, ул. Московская, 2. E-mail: alex_vlasenko@list.ru

ШВЫРЕВ Борис Анатольевич, кандидат физико-математических наук, доцент кафедры компьютерных технологий и информационной безопасности. Кубанский государственный технологический университет. 350000, г. Краснодар, ул. Московская, 2. E-mail: bor2275@yandex.ru

БЕРДНИК Мария Викторовна, доцент кафедры компьютерных технологий и информационной безопасности. Кубанский государственный технологический университет. 350000, г. Краснодар, ул. Московская,2. E-mail: marviktr@mail.ru

VLASENKO Alexandra, Associate Professor, Candidate of Technical Sciences, Head of the Department of Computer Technologies and Information Security. Kuban State Technological University. 350000 Krasnodar, Bld. 2, Moskovskaya street. E-mail: alex_vlasenko@list.ru

SHVYREV Boris, Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Computer Technologies and Information Security. Kuban State Technological University. 350000 Krasnodar, Bld. 2, Moskovskaya street. E-mail: bor2275@yandex.ru

BERDNIK Maria, Associate Professor of the Department of Computer Technologies and Information Security. Kuban State Technological University. 350000 Krasnodar, Bld. 2, Moskovskaya street. E-mail: marviktr@mail.ru

УДК 681.322 Вестник УрФО № 1(27) / 2018, с. 24–28

Баранкова И. И., Михайлова У. В., Лукьянов Г. И.

ПОДХОД К ПРОЕКТИРОВАНИЮ СЕТИ ПРЕДПРИЯТИЯ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

В современном информационном обществе ни одно предприятие или компания не может обойтись без создания собственной корпоративной сети. Такая сеть может быть выполнена как в пределах одного объекта или здания, но чаще применение находят сети с географическим распределением использующие сеть интернет. Передача информации в цифровом виде по сети значительно упрощает доступ злоумышленнику. Кража, изменение и другие действия над информацией злоумшлиником могут нанести значительный ущерб предприятию. В связи с этим безопасность вычислительных корпоративных сетей является важной составляющей современных информационных технологий компьютерной безопасности для любого предприятия. В данной статье рассмотрено проектирование защищенной корпоративной сети предприятия, которое обеспечивает компьютерам данной сети выход в интернет. Разработанная сеть позволяет взаимодействовать филиалам между собой, а так же использовать кроме проводной связи и беспроводную. В спроектированной корпоративной сети обеспечена скорость доступа к интернету на высоком уровне за счет использования высокоскоростных каналов доступа и распределения нагрузки между устройствами. Безопасность спроектированной сети осуществляется за счет применения технологии VLAN, а так же за счет использования списков доступа и AAA-сервера. В зависимости от типа информации и требуемого уровня защиты возможно повышение устойчивости корпоративной сети к атакам из внутренней и внешней сети за счет программных и программно-аппаратных средств защиты информации.

Ключевые слова: *корпоративные сети, безопасность сетей, утечка информации, сетевые атаки, проектирование сетей, каналы доступа, списки доступа, AAA-сервер, VLAN, LAN, ARP-запросы, Ethernet.*

Barankova I. I., Mikhailova U. V., Lukianov G. I.

APPROACH TO THE DESIGN OF THE ENTERPRISE NETWORK IN A PROTECTED DESIGN

In today's information society, no enterprise or company can do without creating its own corporate network. Such a network can be performed as within a single object or building, but more often the use of networks with geographical distribution using the Internet. The transmission of information digitally over the network greatly simplifies access to the attacker. Theft, alteration and other actions on the information by the evil-doer can cause significant damage to the company. In this regard, the security of computing corporate networks is an important

component of modern information technologies of computer security for any enterprise. This article discusses the design of a secure corporate network of the enterprise, which provides computers of the network access to the Internet. The developed network allows branches to interact with each other, as well as use except wired and wireless communication. Designed in the corporate network, provided the speed of Internet access at a high level through the use of high-speed access channels and load balancing between devices. The security of the designed network is carried out through the use of VLAN technology, as well as through the use of access lists and AAA-server. Depending on the type of information and the level of protection required, it is possible to increase the resistance of the corporate network to attacks from the internal and external networks through software and hardware-software information security.

Keywords: *corporate networks, security of networks, information leakage, network attack, network design, access channels, access lists, AAA server, VLAN, LAN, ARPS, Ethernet.*

В современном информационном обществе ни одно предприятие и компания не может обойтись без создания собственной корпоративной сети. Это ускоряет и облегчает работу сотрудников на любом уровне. Но содержит большую угрозу для конфиденциальной информации предприятия. Универсальным средством защиты сети до недавнего времени от нежелательного трафика был межсетевой экран. В настоящее время абсолютную безопасность не может гарантировать ни одна из применяемых технологий [1; 2]. Сетевые атаки становятся год от года все более изощренными, все более активным становится использование методов социальной инженерии. Обеспечение безопасности вычислительных сетей это трудоемкий и сложный процесс, заключающийся в разработке и проведении целого комплекса организационных и технических мероприятий, направленных на достижение следующих целей:

1. Существенное затруднение для злоумышленника возможности произвести сбор информации об интересующей его вычислительной сети [3].

2. Минимизация возможностей для проникновения злоумышленника внутрь охраняемого периметра защищаемой организации и подключения его к локальной вычислительной сети организации [4].

3. Исключение ситуаций возможности перехвата сетевого трафика злоумышленником, если его попытка подключения к локальной вычислительной сети «жертвы» все-таки увенчалась успехом [5].

Первое что необходимо выполнить для обеспечения безопасности проектируемой сети это ее структурирование. Для этого необходимо изучить масштаб предприятия. В данной статье локальная сеть предприятия в защищенном исполнении проектируется для предприятия, в котором имеется два пятиэтажных здания, в каждом из которых находится по семь рабочих групп, по десять рабочих станций в каждой. В процессе проектирования сети предприятия спланирована структура вычислительной сети. Первоначально сегментируется вычислительная сеть, затем определяется схема адресации и осуществляется выбор схемы управления обменом сетевым трафиком между VLAN. Проектирование выполняли в пакете«Ciscopackettracer». Размещение ПК и подключения их к сетевому оборудованию приведены на рис. 1.

Трафик, передаваемый в пределах локальной вычислительной сети, может быть как широковещательным, так и предназначенным конкретному абоненту. При подключении нового компьютера к вычислительной сети Ethernet данный компьютер начинает опрос других компьютеров сети при помощи протокола ARP, рассылая им широковещательные ARP-запросы. Получив от них ответы, компьютер добавляет их MAC-адреса в свою ARP-таблицу. Количество сетевого трафика по протоколу ARP будет превышать все прочие виды трафика, что создаст непроизводительную нагрузку на сетевую инфраструктуру. Более того, обладание информацией обо всех абонентах сети для рядового компьютера в сети является совершенно избыточным. Так же обладание информацией обо всех устройствах сети несет угрозу сетевой безопасности, ибо полномочия сетевых узлов и их пользователей, а также важность обрабатываемой ими информацией и ее характер, могут существенно различаться.

Для устранения вышеперечисленных недостатков сети используем технологии создания виртуальных локальных вычислительных сетей (VLAN). VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети. Такая реорганизация может быть сделана на ос-

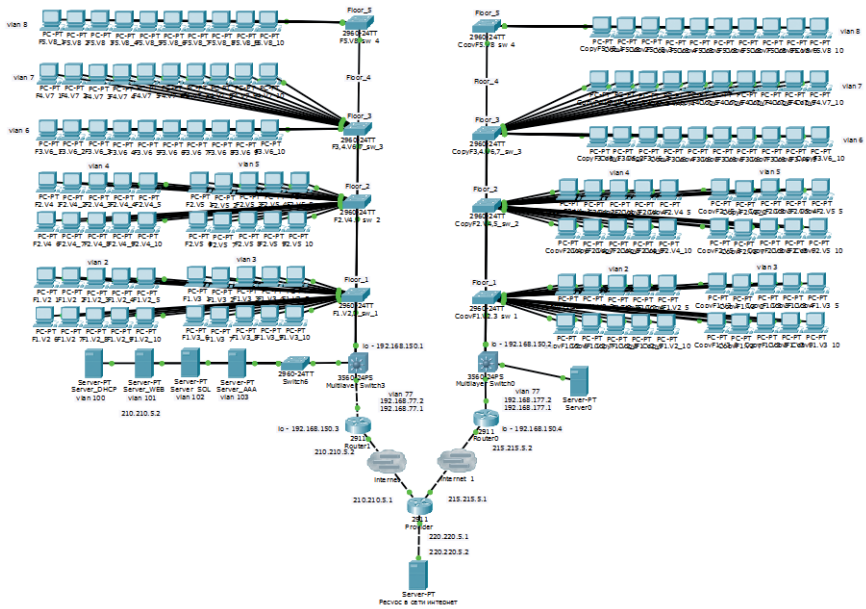


Рис. 1. Схема размещения ПК предприятия и подключения их к сетевому оборудованию

нове программного обеспечения вместо физического перемещения устройств. Согласно данному стандарту, виртуальная ЛВС организуется следующим образом:

1. На сетевых устройствах объявляется виртуальная ЛВС путем задания специальной метки – тэга. Данная метка присваивается сетевым портам коммутаторов ЛВС, к которым подключены группируемые в виртуальную ЛВС сетевые узлы.

2. Сетевой трафик, исходящий от устройств, подключенных к помеченным таким образом портам, маркируется путем присоединения метки VLAN к заголовкам кадров Ethernet. Трафик, тем самым, становится помеченным.

Для этого выполнили настройку VLAN на оборудовании CISCO со всеми рабочими группами на всех коммутаторах второго уровня. Порты которыми коммутаторы второго уровня подключены к коммутаторам третьего уровня сделали trunk портами так как через них будет поступать трафик адресованный к разным устройствам. В результате получили конфигурацию, приведенную на рис. 2.

```
Switch#sho vl br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                 Gig0/2
2    Flor_1_vl_2                       active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11
3    Flor_1_vl_3                       active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

Рис. 2. Конфигурация настроек коммутатора второго уровня

Аналогичные настройки, но с другой нумерацией VLAN'ов проделаны на всех коммутаторах второго уровня.

Коммутатор третьего уровня в отличие от коммутаторов второго уровня осуществляет маршрутизацию трафика с помощью IP адресов. Для этого созданы VLAN'ы для каждой отдельной сети и каждому из них присвоены IP адреса из своей сети. Для динамической маршрутизации с использованием технологии OSPF создан интерфейс локальной петли и перечислены сети к которым существует доступ через этот коммутатор, сделано это для того чтобы не писать отдельно статические маршруты на каждом устройстве. Так же настроен статический маршрут из всех сетей на порт роутера, для выхода в Интернет. Получение IP адресов на ПК осуществляется с помощью выделенного DHCP-сервера. Роутер защитили с помощью пароля, а для дополнительной безопасности использован AAA-сервер. Сервер AAA используется для хранения учетных записей пользователей и дополнительно повышает безопасность и удобство администрирования сети, за счет централизованного управления учетными записями.

Заключение

Описанный в статье подход к проектированию ЛВС предприятия обеспечивает компьютерам данной сети выход в интернет, так же произведена настройка взаимодействия с филиалом, обеспечена скорость доступа к интернету на высоком уровне за счет использо-

вания высокоскоростных каналов доступа и распределения нагрузки между устройствами. Безопасность спроектированной сети осуществляется за счет применения технологии VLAN, а так же за счет использования списков доступа и AAA – сервера. Спроектированная описанным выше образом корпоративная сеть обеспечит оптимально безопасную передачу данных предприятия без использования дополнительных средств защиты информации. В случае необходимости усиленной защиты информации использование специальных средств защиты информации будет обязательным.

Литература

1. Barankova I., Mikhailova U., Lu'yanov G. Automated control system of a factory rail way transport based on ZIGBEE // 2016 2nd International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM – Proseedings. 2016.

2. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. DLP система: защита от утечки информации. Анализ поиска WordSearch // Актуальные проблемы современной науки, техники и образования, 2016. Т. 1. № 1. С. 187-191.

3. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. Прогнозирование локальных и внешних угроз на информационные серверы предприятия // Актуальные проблемы современной науки, техники и образования. – 2017. – Т. 1. С. 217-220.

4. Баранкова И.И., Михайлова У.В., Самохвал В.Д., Огонесян Ш.У Анализ информационных угроз вуза // Актуальные проблемы современной науки, техники и образования. – 2013. – Т. 2. – № 71. С. 157-159.

5. Коновалов М.В., Михайлова У.В., Хусаинов А.А., Санарбаев Р.Ж. Алгоритмы шифрования данных // Актуальные проблемы современной науки, техники и образования. – 2013. – Т. 2. – № 71. С. 159-161.

References

1. Barankova I., Mikhailova U., Lu'yanov G. Automated control system of a factory rail way transport based on ZIGBEE // 2016 2nd International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM – Proseedings. 2016.

2. Barankova I.I, Mikhailova U.V., Lukyanov G.I. DLP sistema: zashchita ot utechki informatsii. Analiz poiska WordSearch[DLP system: protection against information leakage. WordSearch search analysis] // Aktual'nye problemy sovremennoy nauki, tekhniki i obrazovaniya [Actual Problems of Modern Science, Technology and Education], 2016. T. 1. № 1. P. 187-191.

3. Barankova I.I, Mikhailova U.V., Lukyanov G.I. Prognozirovanie lokal'nykh i vneshnikh ugroz na informatsionnye servery predpriyatiya [Forecasting of local and external threats to enterprise information servers] // Aktual'nye problemy sovremennoy nauki, tekhniki i obrazovaniya [Actual Problems of Modern Science, Technology and Education], 2017. T. 1. P. 217-220.

4. Barankova I.I, Mikhailova U.V., Samohval V.D., Oganesyan Sh.U. Analiz informatsionnykh ugroz VUZA [Analysis of information threats of the University] // Aktual'nye problemy sovremennoy nauki, tekhniki i obrazovaniya [Actual Problems of Modern Science, Technology and Education], 2013. T. 2. № 71 P. 157-159.

5. Konovalov M.V., Mikhailova U.V., Husainov A.A., Sanarbaev R.J. Algoritmy shifrovaniya dannykh [Data Encryption Algorithms] // Aktual'nye problemy sovremennoy nauki, tekhniki i obrazovaniya [Actual Problems of Modern Science, Technology and Education], 2013. T. 2. № 71 P. 159-161.

Баранкова Инна Ильинична, доктор технических наук, заведующий кафедрой ИиИБ, Магнитогорский государственный технический университет им. Г. И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: inna_barankova@mail.ru

Михайлова Ульяна Владимировна, кандидат технических наук, доцент кафедры ИиИБ, Магнитогорский государственный технический университет им. Г. И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: ylianapost@gmail.com

Лукьянов Георгий Игоревич, ассистент кафедры ИиИБ Магнитогорский государственный технический университет им. Г. И. Носова 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: decorsi@mail.ru.

Barankova Inna, Department, Nosov Magnitogorsk State Technical University (NMSTU), D. Sc.,Head of Computer Science and Information Safety Engineering (CSISE), Bld. 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: inna_barankova@mail.ru;

Mikhailova Uliana, NMSTU, Ph.D.,Associate Professor of CSISE Department, Bld. 38, Lenina Ave,

Magnitogorsk, Russia, 455000, E-mail: ylianapost@gmail.com;

Lukianov Georgy, NMSTU, Teaching Assistant of CSISE Department, Bld. 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: decorsi@mail.ru.

УДК **629.3.064.5 + 004.056** Вестник УрФО № 1(27) / 2018, с. 29–33

Синьков А. С., Лужнов В. С.

АНАЛИЗ БЕЗОПАСНОСТИ CAN-ШИНЫ ТРАНСПОРТНЫХ СРЕДСТВ

Безопасность представляет собой фундаментальную проблему в современных транспортных средствах. В них добавляются множество систем, включающих электронные блоки управления, которые связаны между собой системной шиной – Controller Area Network (CAN), являющейся самой важной частью автомобиля. Она основана на протоколе CAN, который не обеспечивает должной безопасности, что показано в данной статье. В статье содержится описание самого протокола и основных принципов его функционирования. Также рассмотрены возможные сценарии атак, которые позволяют злонамеренным злоумышленникам препятствовать системам управления автомобилем и наносить вред автомобилю даже пассажирам, их виды и устройства, с помощью которых их возможно осуществить. Выделены меры защиты транспортных средств от взлома CAN-шины.

Ключевые слова*: Информационная безопасность, CAN-шина, безопасность автомобильных систем, Controller Area Network, безопасность транспортных средств.*

Sinkov A. S., Luzhnov V. S.

SECURITY ANALYSIS OF CAN-BUS VEHICLES

Safety is a fundamental problem in modern vehicles. In cars, many systems are added, including electronic control units, which are connected by a system bus – the Controller Area Network (CAN), which is the most important part of the car. It is based on the CAN protocol, which does not provide the necessary security, as shown in this article. The article contains a description of the protocol itself and the basic principles of its functioning. Also considered are possible attack scenarios that allow malicious cybercriminals to interfere with vehicle control systems and damage the car even to passengers, their types and devices by which they can be carried out. Measures to protect vehicles from hacking CAN bus.

Keywords*: Information security, CAN-bus, safety of automobile systems, Controller Area Network, safety of vehicles.*

Увеличение сложности технологий, внедряемых в современные автомобили растёт с каждым годом, что увеличивает их функциональность, но одновременно с этим и несет все больше уязвимостей в безопасности. Злоумышленники могут злоупотреблять найденными уязвимостями и наносить вред самому автомобилю, а также пассажирам.

В современных транспортных средствах устанавливается ряд электронных блоков управления (ЭБУ), которые управляют различными функциями автомобиля. Все они

связаны между собой системной шиной контроллера (CAN – Controller Area Network). Она имеет протокол для последовательной связи, обеспечивает достаточно высокий уровень безопасности и поддерживает распределенное управление электронными блоками управления (ECU) в реальном времени [1]. При этом протокол CAN не обеспечивает конфиденциальности и аутентификации для кадров, пересылаемых по шине. CAN-шина передает информацию кадрами, которые транслируются сразу во всю сеть, что сразу же вызывает много проблем безопасности, таких как перехват.

Преимущества при использовании CAN протокола:

– обеспечивает большую скорость передачи (до 1 Мбит/с);

– протокол CAN успешно реализован в системах реального времени;

– обеспечивает хорошее соотношение производительности и цены;

– информация передается сразу всем узлам сети короткими кадрами;

– надежный контроль за ошибками передачи и приема;

– высокая устойчивость к помехам.

Существует 4 типа CAN-сообщений:

– кадр данных (Data Frame) – стандартное сообщение;

– кадр запроса передачи (Remote Frame) – это Data Frame, но без поля с данными, чаще всего необходимы для запроса передачи данных;

– кадр ошибки (Error Frame) – передается узлом при нарушении формата принятого сообщения;

– кадр перегрузки (Overload Frame) – используется перегруженным узлом для просьбы повтора сообщения.

Распространены несколько версий протокола: CAN 2.0A и CAN 2.0B, последний также именуется, как Extended CAN. Они отличаются размерами кадров и скоростями передачи. В таблице представлены кадры для стандартной версии протокола (2.0A) и расширенной (2.0B) [1]. В стандарте 2.0B скорость передачи варьируется в диапазоне от 125 Кбит/с до 1 Мбит/с, ее определяет, в большей степени, дина кабеля. Максимальная скорость обеспечивается в сети до 40 метров [1]. В тоже время в стандарте 2.0A максимальная скорость: 125 Кбит/с.

Кадр данных для 2.0A и 2.0B

Поле	Длина (бит) для 2.0A	Длина (бит) для 2.0B	Описание
Начало кадра (SOF)	1	1	Указывается доминантный бит
Базовый идентификатор	11	11	Уникальный идентификатор, определяющий приоритет
Бит подмены запроса на передачу (SRR)	Поле отсутствует	1	Рецессивный бит
Поле расширения идентификатора	Поле отсутствует	18	Расширение поля арбитража для расширенного формата
Удаленный запрос передачи (RTR)	1	2	Доминантный бит в поле данных для 2.0A и рецессивные биты для 2.0B (для Remote Frame – индикатор получения)
Зарезервированное	2	Поле отсутствует	Доминантные биты
Код длины данных (DLC)	4	4	Число байт в поле данных (0-8)
Поле данных	0-8 байт	0-8 байт	Длина определяется полем DLC
Поле циклического контроля избыточности (CRC)	15	15	Контрольная последовательность, формируемая БЧХ-кодом (до 127 бит)
Разделитель CRC	1	1	Должен быть рецессивным битом
Поле подтверждение приема (ACK)	1	1	Отправитель записывает рецессивный бит, получатель – доминантный бит
Разделитель ACK	1	1	Должен быть рецессивным битом
Конец кадра (EOF)	7	7	Состоит из рецессивных битов
Итого без поля данных, бит:	45	62	

Стоит отметить, что, используемые в таблице термины рецессивный и доминантный, описывают двоичные состояния «0» и «1» соответственно.

Порядок передачи битов в кадре данных для версий протокола 2.0A и 2.0B представлены на рис. 1.

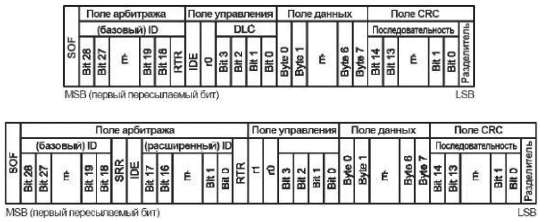


Рис. 1. Порядок передачи битов (сверху – базовый формат 2.0A, снизу – расширенный 2.0B)

При получении доступа к CAN-шине (например, через диагностический разъем ODB-II [2]), злоумышленник может совершать различные действия с автомобилем, вплоть до полной его остановки, что может привести к катастрофическим последствиям.

ЭБУ соединены друг с другом на нескольких шинах, соответствующих спецификациям CAN. Связь осуществляется между ЭБУ путем отправки CAN-пакетов. Компоненты не могут определить откуда прибыл пакет CAN, поскольку протокол не поддерживают какую-либо форму аутентификации, поэтому легко для любого пакетного сниффера перехватывать исходный пакет, маскировать как законный пакет или отправлять ложные данные в CAN-пакеты. Из-за отсутствия аутентификации, обратная трассировка скомпрометированного ЭБУ, который отправляет вредоносные атакующие пакеты на CAN, практически невозможна в режиме реального времени [3]. В связи с этим возникает возможность, отслеживая сеть CAN и ЭБУ, генерировать ложные сообщения, чтобы ЭБУ инициировал выполнение определенного действия.

Подключится к CAN-шине автомобиля для получения сообщений можно, например, с помощью двуканального осциллографа. Необходимо найти витую пару, принадлежащая CAN-шине и снимать с них сигнал. Однако наиболее простой способ подключение к CAN-шине автомобиля – через порт OBD-II. Данный разъем устанавливается во все современные транспортные средства. Основная его цель – диагностика обслуживания двигателя и транспортных средств. Наиболее популярные устройства, подключаемые к данном порту: ELM327, CARDAQ-Plus, Launch CReader и др. Также существует устройство CANCrocodile (рис. 2), которое подключится к витой паре автомобиля без нарушения оплетки проводов, т. е. считывание происходит без физического контакта с проводами [4]. Оно изначально предназначалось для подключения к шине CAN систем GPS/ГЛОНАСС мониторинга, однако возможно и подключение, например, к компьютеру посредствам дополнительного устройства MasterCAN Tool, который считывает и анализирует данные с шины.

Рис. 2. Устройства для подключения к CAN-шине (слева направо: CANCrocodile, ELM327, Launch CReader)

Для отправки пакетов через CAN-шину можно воспользоваться готовым адаптером, например, ELM327, либо собрать собственный адаптер, например, из Arduino Uno, микрочипа MCP2551 и разъема SAE J1962 [5].

Возможные сценарии атаки

Узлы в сети CAN могут использовать энергозависимую (RAM) и (или) энергонезависимую (flash) память. Любой узел может быть, как отправителем сообщений, так и получателем.

Как уже упоминалось, CAN-шина не имеет никакой аутентификации. Поэтому, если злоумышленнику удастся получить доступ к шине, он может получить код, запущенный на ЭБУ. Кроме того, он может полностью управлять автомобилем, отправляя поддельные сообщения. В связи с этим, возможны несколько сценариев получения доступа к CAN-шине транспортного средства с целью отправки сообщений:

– Сценарий 1: злоумышленник использует дополнительное внешнее устройство для доступа к шине, присоединив его, например, к диагностическому порту OBD-II.

– Сценарий 2: злоумышленник получил доступ к сети CAN, скомпрометировав один из существующих ЭБУ автомобиля.

– Сценарий 3: если автомобиль оснащен доступом в сеть Интернет, то злоумышленник, обойдя штатную систему защиты, может получить доступ к шине.

Последний сценарий атак наиболее привлекателен для злоумышленников, поскольку нет необходимости непосредственной модификации систем автомобиля, будь то компрометация ЭБУ или установка OBD-II устройства, а также в связи с возрастанием интегрированности сети Интернет, необходимого для удаленного диагностики, тематики. В частности, транспортные средства марки Tesls используют Интернет-соединение для обновления внутренних систем автомобиля [6].

После получения доступа к CAN-шине автомобиля, злоумышленник может либо отправлять поддельные сообщения, либо повторно посылать прослушанные сообщения [7].

При атаке с отправкой фальшивых сообщений, противник пытается отправить поддельное сообщение, заявив себя в качестве другого ЭБУ, то есть используя отличный идентификатор узла от назначенного ему в сообщении аутентификации.

Возможно, также, полностью отключить какой-то узел от шины путем отправки большого количества ошибочных кадров, связанных с определенным узлом, после чего узел отключается от общей шины [5]. Таким образом можно отключить важные системы автомобиля, путем штатного механизма обработки ошибок протокола CAN, не позволяющей влиять отказавшим узлам на работу всей системы.

Для второго вида атак (дублирование сообщений) первоначально злоумышленнику необходимо некоторое время считывать сообщения, пересылаемые, между блоками и выделить среди них необходимые. Поскольку протокол CAN не поддерживает аутентификацию сообщения, ЭБУ-получатель не может идентифицировать данные в сообщении и выполняет функцию, которая находится в пакете CAN. Например, если злоумышленник хочет атаковать тормоза транспортного средства, он должен непрерывно отправлять пакет, вызывающий блокировку тормозных дисков.

В качестве примера, рассмотрим автомобиль Ford Escape [7]. Чтобы остановить двигатель, а точнее, блокировать цилиндры, достаточно непрерывно отправлять пакеты вида: IDH: 30, IDL: F5, Len: 08, Data: FF FF FF FF FF FF FF FF. Также имеется возможность изменить показания спидометра, посылая ложные пакеты по CAN-шине. Возможно отключение всех осветительных приборов в автомобиле (для выключения требуется, чтобы он не был в движении) и даже тормозной системы, путем отправки команды 0x003C [3].

Способы защиты

Наиболее кардинальный и действенный способ защиты – это отключение всех систем, использующих Интернет-соединение и ограничение круга лиц, которые имеют доступ к автомобилю, и слежение за действиями людей, допущенных к нему, для избегания установки дополнительных устройств, подключаемых к CAN-шине.

В настоящее время широко применяют шифрование данных. Так, для защиты системы достаточно шифровать отправляемые сообщения каждым ЭБУ, однако при таком подходе теряется скорость обмена сообщениями.

Для защиты от 3 сценария атак разрабатываются блоки управления шлюзом связи, который защищает внутренние системы автомобиля от внешней среды. Так, компании Kaspersky и AVL создали прототип такого устройства – модуль безопасного соединения (Secure Communication Unit – SCU) [8]. Данное устройство позволяет обмениваться блокам внутри автомобильной сети в обход SCU, что положительно сказывается на скорости работы.

Литература

1. ГОСТ Р ИСО 11898-1-2015. Транспорт дорожный. Местная контроллерная сеть (CAN). Часть 1. Канальный уровень и передача сигналов.

2. Carsten P., Andel T.R., Yampolskiy M., McDonald JT. In-vehicle networks: attacks, vulnerabilities, and proposed solutions. In: Proceedings of the 10th annual cy- ber and information security research conference. ACM; 2015. p. 1.

3. Miller C., Valasek C. Adventures in automotive networks and control units. Def Con 2013; Volume 21, p.260–264.

4 CANCrocodile безопасное получение данных CAN шины // Технотон. URL: http://www.technoton.by/crocodile/cancrocodile (дата обращения 10.12.2017).

5. Palanca A., Evenchick E., Maggi F., Zanero S. A Stealth, Selective, Link-Layer Denial-of-Service Attack Against Automotive Networks // Springer International Publishing. 2017. Vol. 10327. P. 185-206. doi: 10.1007/978-3-319-60876-1

6. Software updates // Tesla. URL:https://www.tesla.com/support/software-updates (дата обращения 25.12.2017).

7. Wang Q., Sawhney S. Vecure: a practical security framework to protect the can bus of vehicles. In: Internet of Things (IOT), 2014 international conference on the. IEEE; 2014. p. 13–18.

8. Умный автомобиль – безопасный автомобиль: «Лаборатория Касперского» и AVL представили модуль для киберзащиты для современных машин // Kaspersky lab. URL: https://www.kaspersky.ru/about/press-releases/2017_kaspersky-lab-and-avl-presented-module-for-cyber-defense-for-modern-machines (дата обращения 22.12.2017)

References

1. GOST R ISO 11898-1-2015. Transport dorozhnyj. Mestnaja kon-trollernaja set' (CAN). Chast' 1. Kanal'nyj uroven' i peredacha signalov.

2. Carsten P., Andel T.R., Yampolskiy M., McDonald JT. In-vehicle net-works: attacks, vulnerabilities, and proposed solutions. In: Proceedings of the 10th annual cy- ber and information security research conference. ACM; 2015. p. 1.

3. Miller C., Valasek C. Adventures in automotive networks and control units. Def Con 2013; Volume 21, p.260–264.

4 CANCrocodile bezopasnoe poluchenie dannyh CAN shiny // Tehnoton. URL: http://www.technoton.by/crocodile/cancrocodile (data obrashhenija 10.12.2017).

5. Palanca A., Evenchick E., Maggi F., Zanero S. A Stealth, Selective, Link-Layer Denial-of-Service Attack Against Automotive Networks // Springer Inter-national Publishing. 2017. Vol. 10327. P. 185-206. doi: 10.1007/978-3-319-60876-1

6. Software updates // Tesla. URL:https://www.tesla.com/support/software-updates (data obrashhenija 25.12.2017).

7. Wang Q., Sawhney S. Vecure: a practical security framework to protect the can bus of vehicles. In: Internet of Things (IOT), 2014 international confer-ence on the. IEEE; 2014. p. 13–18.

8. Umnyj avtomobil' – bezopasnyj avtomobil': «Laboratorija Kas-perskogo» i AVL predstavili modul' dlja kiberzashhity dlja sovremennyh mashin // Kaspersky lab. URL: https://www.kaspersky.ru/about/press-releases/2017_kaspersky-lab-and-avl-presented-module-for-cyber-defense-for-modern-machines (data obrashhenija 22.12.2017)

СИНЬКОВ Антон Сергеевич, студент кафедры защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, пр. Ленина, д. 76. E-mail: sinkov_96@mail.ru

ЛУЖНОВ Василий Сергеевич, ассистент кафедры защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, пр. Ленина, д. 76. E-mail: ua9stz@gmail.com

SINKOV Anton, student of the department of information security of the school of electrical engineering and computer science «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: sinkov_96@mail.ru

LUZHNOV Vasiliy, Assistant of the Information Security Department of the Higher School of Electronics and Computer Science "South Ural State University (National Research University)". 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: ua9stz@gmail.com

УДК 004.056 Вестник УрФО № 1(27) / 2018, с. 34–41

Дресвянин П. Д., Сафиуллин Н. Т., Поршнев С. В.

О ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ АЛГОРИТМА ЭМПИРИЧЕСКОЙ МОДОВОЙ ДЕКОМПОЗИЦИИ ДЛЯ ИДЕНТИФИКАЦИИ АВТОРА РЕЧЕВОГО СИГНАЛА

В статье проводится анализ проблем, связанных с идентификацией источников акустических сигналов в случае их использовании в качестве паролей при авторизации пользователей интеллектуальных информационных систем (ИС). Приведен обзор актуальных решений, основанных на использовании биометрических показателей, а также обоснован выбор направления их дальнейшего развития в России. Особое внимание уделено необходимости обеспечения информационной безопасности (ИБ) данных решений в связи с активным развитием методов атак на компьютерные технологии, использующие методологии машинного обучения и искусственных нейронных сетей. Предложена новая методика идентификации речевых сигналов, основанная на использовании эмпирической модовой декомпозиции (метода преобразования Хуанга-Гильберта), в которой для идентификации автора цифрового звукового сигнала используется коэффициент линейной корреляции между модами, выделенными в результате его декомпозиции. Продемонстрировано, что предложенная методика достаточно устойчива к шумам, присутствующим в речевом сигнале, и вариациям его длительности.

Ключевые слова: *эмпирическая модовая декомпозиция, идентификация, биометрическая авторизация, цифровая обработка сигналов, голосовой пароль.*

ON THE POSSIBILITY TO USE EMPIRICAL MODE DECOMPOSITION TECHNIQUE FOR SPEECH IDENTIFICATION

The article analyses the issues of speech identification – the process that underlies the biometric voice-password authorization in intellectual informational systems. The actual methods of biometric authorization, based on machine learning and artificial neural networks, are presented; the direction of their development and their necessity for Russia are specified in the paper. Special accent made on the necessity of providing informational security for such tasks due to the development of methods for attacks on identification procedures, specifically based on machine learning and artificial neural network techniques. Because of the analysis, the authors provide an alternative technique for speech identification in biometric authorization intellectual systems by using empirical mode decomposition. The paper shows the possibility of using the linear correlation coefficient between identical (by number) intrinsic modes, received by decomposition, as a measure for one-valued recognition, required for authorization. The authors demonstrate that the proposed technique is quite stable and robust in case of noise and other perturbations of digital speech signal. The complexity and accuracy of this technique can be increased by using time-and-frequency analysis of the received intrinsic modes – an issue, which is scheduled for a future research.

Keywords*: empirical mode decomposition, identification, biometric authorization, digital signal processing, voice password.*

Введение

Интеллектуальные интерфейсы, обеспечивающие на основе идентификации речевого сигнала взаимодействие между пользователем и той или иной технической системой, в настоящее время находят применение в различных областях науки и техники. Отметим, что, если на начальном этапе применения подобные системы рассматривались исключительно как дополнительное средство ввода команд голосом, то теперь распознавание речи является неотъемлемой частью методов авторизации пользователей с помощью биометрических показателей [1]. Данная ситуация способствует быстрому развитию информационных технологий (ИТ) в данной области [2], что подтверждается наличием большого числа программных инструментов в сегменте речевых помощников (Google Now, Amazon Alexa, Яндекс Алиса и др.). Также отметим, что, например, в планах департамента финансовых и ИТ Банка России запланировано использование цифрового профиля пользователя, в котором будут интегрированы биометрические данные и образцы голоса, что обеспечит возможность удаленной идентификации пользователей для обеспечения его доступа к таким видам услуг как страховые, пенсионные и нотариальные [3]. При этом понято, что подобная идентификация пользователей цифрового профиля на основе биометрических данных и образца голоса обеспечивает значительное повышение ИБ соответствующих автоматизированных интеллектуальных систем. Отметим, что данные решения в дальнейшем можно будет тиражировать, в том числе, в сферу государственных и муниципальных цифровых услуг, что особенно актуально, принимая во внимание Постановление Правительства РФ от 24.10.2011 № 861 (ред. от 10.02.2018) «О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций)».

В области идентификации параметров речевых сигналов приходится решать задачи, отличающиеся друг от друга своей постановкой.

Например, при разработке тех или иных речевых помощников наиболее актуальной оказывается задача точного распознавания слов, их верного семантического истолкования и извлечения информации из ключевых фраз [2]. В тоже время для систем защиты информации на основе биометрических показателей необходимо установить взаимно однозначное соответствие между данным речевым сигналом и конечным пользователем. При этом, как при решении первой, так и второй задачи, необходимо учитывать, что частотно-временные характеристики любого речевого сигнала обладают высокой вариабельностью, следствием которой оказывается его нестационарность, кроме того в речевых сигналах присутствует шум, как правило, с неизвестной функцией распределения. Отмеченные обстоятельства, вообще говоря, ставят по сомнение правомерность использования стандартные статистические или спектральные методы, необходимым условием применения которых является стационарность анализируемого сигнала [4].

В этой связи поиск новых подходов к решению задачи идентификации речевых сигналов – установления однозначного соответствия между сохраненным в системе доступа речевым паролем и акустическим сигналов, зарегистрированным при его повторном произнесении пароля в других условиях и, соответственно, с возможными искажениями, – является актуальной и обладает несомненной практической ценностью для систем ИБ на основе считывания биометрических показателей.

В настоящее время из-за теоретических ограничений, возникающих при использовании известных спектральных и статистических методов для анализа нестационарных временных рядов, к которым относятся и речевые сигналы, продолжается активный поиск альтернативных методов оценивания их частотно-временных характеристик. В области речевых помощников такой альтернативой стали методы машинного обучения и нейронные сети [2; 5], в которых задачу установления однозначного соответствия между речевым сигналом и некоторым семантическим ключом возлагают на автоматизированные средства поиска оптимального решения (например, при обучении нейронных сетей с обратным градиентным распространением ошибки). Получившийся «черный ящик» содержит в себе невидимые для конечного пользователя зависимости и коэффициенты, формирующие для заданного речевого сигнала некоторый ключ, обеспечивающий в дальнейшем его идентификацию. Каждый из методов, базирующихся на машинном обучении, работает по принципу «фразы-пароля» или «фразы-ключа», поскольку в данных методах изначально отсутствуют средства анализа частотно-временных характеристик речевых сигналов. Однако в силу обобщающей способности подобных алгоритмов они оказываются устойчивыми к шуму и изменениям тембра/тона голоса.

С точки зрения требований ИБ к системам опознавания по голосу, методы, основанные на использовании алгоритмов машинного обучения, обладают существенным недостатком – их входные данные можно подделать таким образом, чтобы получить выходной оптимальный результат даже без знания необходимого ключа. Это обусловлено тем, что конечные связи и коэффициенты найденного машинного решения не могут быть найдены непосредственно из исходной информации напрямую, а калибруются в ходе обобщающего обучения, что приводит к невозможности четкого сопоставления исходной информации с конечным результатом [6].

Подобный недостаток был продемонстрирован на примере задачи классификации изображений на основе алгоритмов искусственных нейронных сетей с помощью атак вида «черный ящик» [7]. Здесь задача классификации изображения состояла в отнесении данного изображения с заданным уровнем достоверности к соответствующему классу или установление соответствия между изображением и некоторым термином (например, названием вида животного). В [7] было показано, что существует некоторая пиксельная маска, при наложении которой на это изображение обученная нейронная сеть будет распознавать уже другой класс понятий. Более того, оказывается возможным наложить на любое изображение такую маску, которая обеспечит заранее ожидаемый результат, то есть фальсификацию ключа. При этом с точки зрения человека, что наиболее важно, изображение не претерпевает существенных изменений, но результат, возращенный обученной искусственной нейронной сетью, в данном случае оказывается совершенно неожиданным. Отметим, что подобных примеров «обмана» нейронных сетей в задачах распознавания речевых сигналов пока не опублико-

вано. Однако наличие такой потенциальной возможности заставляет усомниться в возможности применения данной методики в области ИБ.

Альтернативой методам машинного обучения могут служить адаптивные методы анализа цифровой информации, не накладывающие на исходный сигнал никаких ограничений по его статистическим, спектральным и прочим характеристикам. Одним их таких относительно новых методов является Преобразование Хуанга-Гильберта [8], созданное Н. Хуангом в 1998 г., и состоящее из двух этапов. На первом этапе выполняется эмпирическая модовая декомпозиция (ЭМД) исходного сигнала на компоненты, содержащие ключевые параметры исходного сигнала. На втором этапе с помощью преобразования Гильберта или построения Гильбертова спектра определяются частотно-временные характеристики выделенных компонент и сигнала в целом. Далее в нашей статье будет продемонстрировано, что информации, выделенной с помощью метода ЭМД, оказывается достаточно для идентификации речевых сигналов, то есть для установления взаимно-однозначного соответствия между исходным речевым паролем и его последующим произношением в других условиях, в том числе, с искажениями. Расчет частотно-временных характеристик и выделение из них ключевых параметров речевого сигнала не рассматривались, так как являются более широкой задачей, для которой требуются дополнительные исследования.

Основные сведения о методе ЭМД

Напомним, что метод ЭМД является эмпирическим алгоритмом, который не предъявляет к исходному временному ряду (ВР) требований о стационарности его характеристик, но требует, чтобы значения ВР были заданы в узлах равномерной временной сетки. В основе метода ЭМД лежит построение интерполяционных огибающих кривых ВР, проходящих через локальные максимумы/минимумы ряда, с последующим устранением их среднего из анализируемого сигнала до тех пор, пока остаток не будет удовлетворять некоторому условию, после чего он принимается за компоненту. Метод строится итерационно, что позволяет разложить исходный сигнал в аддитивную сумму характеристических компонент, лежащих в разных частотных областях [8]. Блок-схема полного алгоритма, подробно описанного в [12], представлена на рис. 1.

Несмотря на первые успешные результаты, полученные с помощью данного метода при анализе различных цифровых сигналов [8], ЭМД обладала двумя существенными недостатками: низкой точностью разделения

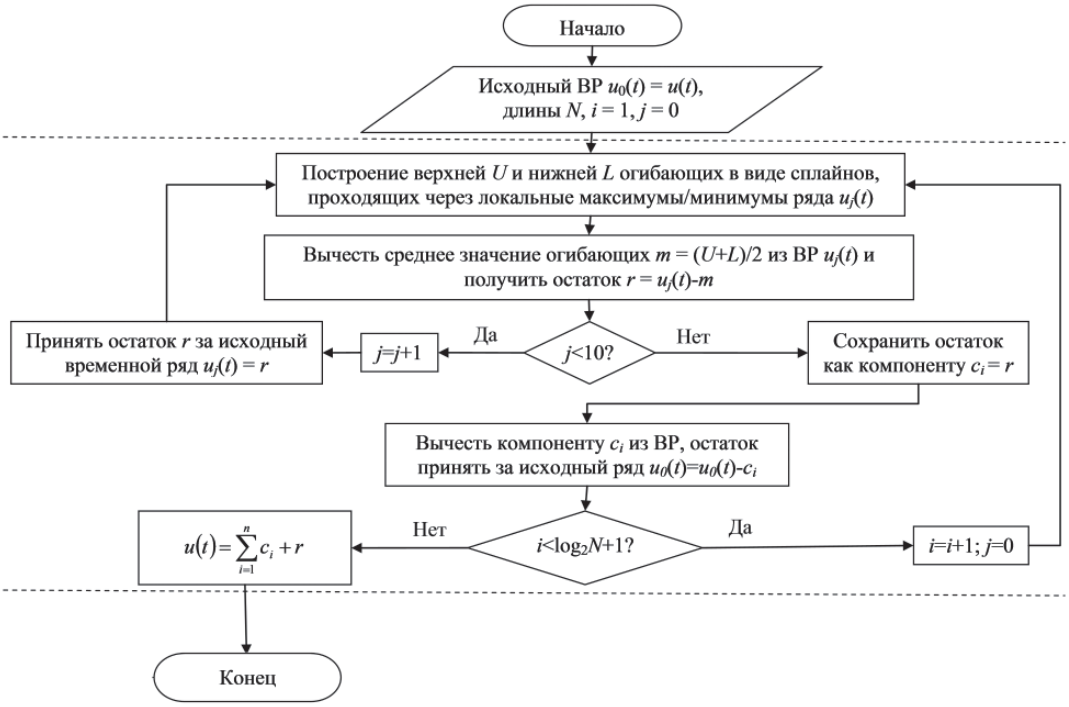


Рис. 1. Блок-схема алгоритма эмпирической модовой декомпозиции (ЭМД)

компонент при наличии в исходном сигнале шума большой мощности [9] и низкой скоростью вычислительного алгоритма в целом [8]. Однако в последние годы в алгоритм ЭМД были внесены существенные изменения. Исходная декомпозиция была доработана до комплементарной ансамблевой эмпирической модовой декомпозиции (CEEMD) [10], которая обеспечила существенное повышение устойчивости метода к шуму. Также удалось достичь значительного сокращения времени вычислений ЭМД, зависящего, однако, от архитектуры его конкретной программной реализации [11], в том числе при использовании технологий параллельных вычислений [12]. Таким образом, сегодня метод ЭМД, в том числе как составная часть Преобразования Хуанга-Гильберта, является инструментом, готовым к использованию для анализа временных рядов и цифровых сигналов.

Методика проведения исследования

Исследование возможности идентификации речевых сигналов на основе метода ЭМД проведено в соответствие с методикой, реализующейся выполнением следующей последовательности действий:

Декомпозиция исходного речевого сигнала *y* длины *T* с частотой дискретизации f_d с помощью метода CEEMD (модификации ЭМД [11; 12]) на характеристические компоненты F_i, общее число которых *N* фиксировано

и известно заранее: $y = \sum_{i=1}^{N} F_i$.

Выбор одной из выделенных компонент анализируемого сигнала для идентификации речевого сигнала. Номер этой компоненты *K* и ее отсчеты временного ряда F_K являются необходимым цифровым ключом $\{K, F_K\}$ для идентификации речевого сигнала. В дальнейшем планируется проверка гипотезы о возможности хранения не самих отсчетов речевого сигнала, а только некоторых его характеристик, по которым можно будет установить однозначное соответствие между ключом и считываемым речевым сигналом.

Выбор некоторого нового речевого сигнала *x*, в качестве претендента на идентификацию в качестве ключа, представляющего собой временной ряд близкой длины, значения которого заданы в узлах временной сетки с такой же частотой дискретизации f_d.

Декомпозиция временного ряда *x* с помощью метода CEEMD на характеристические компоненты G_i, G_i, $x = \sum_{i=1}^{N} G_i$, при этом общее число компонент *N* выбирается таким же, как и у исходного сигнала-пароля *y*.

Сравнение компоненты G_K с номером *K* с соответствующей компонентой-ключом F_K путем вычисления коэффициента корреляции Пирсона. При значении этого коэффициента выше некоторого порогового значения, речевой сигнал *x* принимается за действительный ключ, тем самым подтверждая его идентификацию. В обратном случае речевой образец *x* отвергается, и авторизация не проходит.

Выбор коэффициента корреляции Пирсона для оценивания соответствия компонент F_K и G_K обусловлен его достаточной устойчивостью к временному сдвигу сигналов. Далее будет продемонстрировано, что даже такой простой характеристики оказывается достаточно для подобной задачи с учетом использования алгоритма ЭМД. В дальнейшем планируется усложнение алгоритма с использованием частотно-временных характеристик компонент в качестве ключевых параметров для идентификации соответствующего цифрового ключа.

Анализ экспериментальных результатов

Описанная выше методика исследований была апробирована на стандартном речевом сигнале «speech_dft», из аудио-библиотеки образцов MATLAB Audio System Toolbox. Данный речевой образец содержит запись мужского голоса хорошего качества без существенных помех, длина сигнала 5.1199 секунд, частота дискретизации 22 500 Гц, используется только один аудиоканал (моно-запись).

В аудио-библиотеке MATLAB Audio System Toolbox также имеется готовый искаженный этот же речевой образец худшего качества с высокоуровневым шумом мощности 5 дБ, длина сигнала отличается несущественно (5.0175 секунд), частота дискретизации 22 500 Гц, используется только один аудиоканал (моно-запись). Данные сигналы представлены на рис. 2. Также исходный речевой сигнал для расширенного тестирования предложенного алгоритма искажался вручную следующими способами: наложением шума разной мощности (от 2 до 20 дБ); сокращением общей длины сигнала в меньшую сторону (до 20 %). Коэффициент корреляции между исходным речевым сигналом и его искаженными вариантами не превышает значения в 0.65.

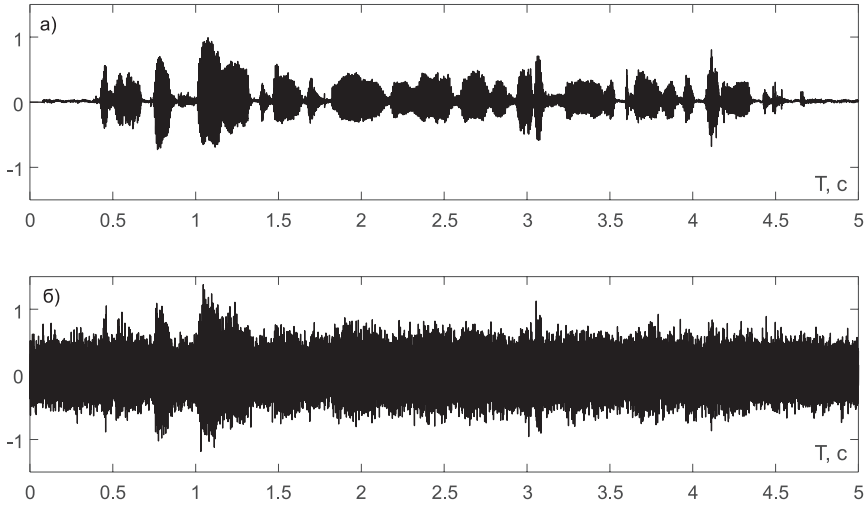


Рис. 2. Исходный речевой сигнал (а) и искаженный сигнал (б)

Результаты пробной идентификации для различных номеров компонент приведены в таблице. Пороговое значение коэффициента корреляции Пирсона для однозначной идентификации было выбрано уровнем выше 0.90.

Средний коэффициент корреляции между характеристической компонентой с номером *K* исходного речевого образца и его искажения

Номер компоненты	Искаженный сигнал (рис. 2б)	Искажение сигнала шумом	Искажение сигнала по длине
1	0.4843	0.2523	0.5002
2	0.4345	0.1291	0.4474
3	0.6970	0.5309	0.7074
4	**0.9760**	**0.9618**	**0.9547**
5	**0.9166**	0.8309	**0.9070**

Из таблицы видно, что в качестве характеристической компоненты для идентификации данного речевого образца лучше всего выбирать компоненту с номером $K = 4$, так как она оказывается наиболее устойчивой ко всем искажениям и обладает наибольшим коэффициентом корреляции между исходным речевым ключом и пробным речевым сигналом.

Компоненты № 4 для исходного речевого сигнала (а) и для искаженного сигнала (б) приведены на рис. 3. Из рис. 3 даже визуально видно, что выделенные компоненты весьма похожи друг на друга.

Также для проверки данного алгоритма проведено сравнение исходного речевого сигнала с другими речевыми рядами (другими фразами) той же длины T с той же частотой дискретизации f_d. Во всех случаях и по всем компонентам коэффициент корреляции не

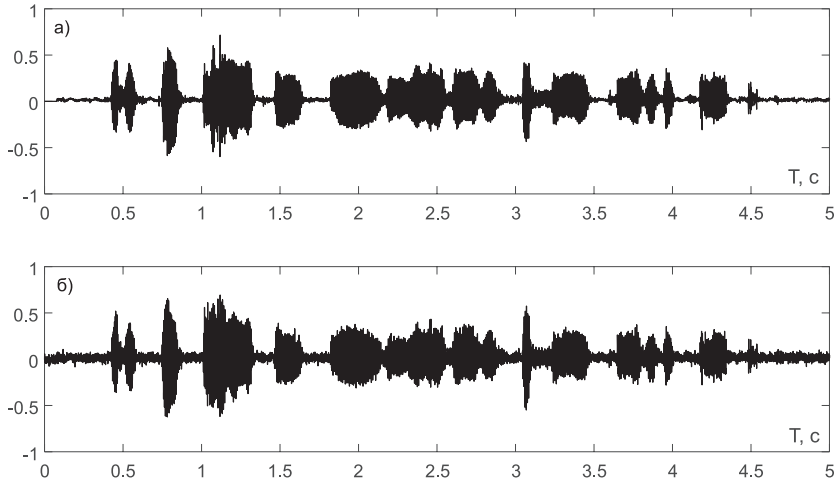


Рис. 3. Компонента под номером $K = 4$ для исходного речевого сигнала (а) и для искаженного сигнала (б)

превысил 0.60, то есть оказывался существенно ниже ожидаемого порогового значения, тем самым обеспечивая некоторую устойчивость к подбору идентификационного ключа.

Таким образом, результаты проведенных экспериментальных исследований предложенной методики подтвердили ее работоспособность. Далее авторы планируют проверить ее устойчивость и точность при использовании различных слов-ключей и различных уровнях акустических помех.

Заключение

Предложена методика идентификации речевых сигналов, использующихся в качестве биометрического пароля доступа к интеллектуальным информационных системам, основанная на методе эмпирической модовой декомпозиции.

Обосновано, что данная методика устойчива к атакам типа «черный ящик» [7].

Приведены экспериментальные результаты, подтверждающие ее работоспособность.

Определены направления дальнейших исследований, цель которых состоит в автоматизации выбора наиболее информативной с точки зрения решаемой задачи компоненты речевого сигнала, а также повышении точности и устойчивости разработанной методики, результаты которых станут предметом последующих публикаций.

Примечания

1. Shari Trewin, etc. Biometric authentication on a mobile device: a study of user effort, error and task disruption. In Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC '12). ACM, New York, NY, USA, – 2012. – pp. 159–168. DOI:10.1145/2420950.2420976

2. Alisa Kongthon, etc. Implementing an online help desk system based on conversational agent. In Proceedings of the International Conference on Management of Emergent Digital EcoSystems (MEDES '09). ACM, New York, NY, USA, – No. 69, – 2009. DOI:10.1145/1643823.1643908

3. Российская газета. Федеральный выпуск №7515 (52). [Электронный ресурс] https://rg.ru/2018/03/13/rossiiane-smogut-brat-kredity-i-otkryvat-vklady-po-vneshnosti-i-golosu.html (Дата обращения 28.03.2018)

4. Сергиенко А. Б. Цифровая обработка сигналов. – 2-е. изд. – СПб. : Питер 2007. – С. 751.

5. Tur, G., De Mori R., Spoken Language Understanding: Systems for Extracting Semantic Information from Speech. – John Wiley & Sons, Ltd – 23 March 2011. – 450 p. DOI: 10.1002/9781119992691

6. M. Hagan, H. Demuth, M. Beale. Neural Network Design. – Amazon Publ. 2nd ed. – 2016. – 1012 p.

7. Nicolas Papernot, Patrick McDaniel, Ian Goodfellow, Somesh Jha, Z. Berkay Celik, Ananthram Swami. Practical Black-Box Attacks against Machine Learning. Proceedings of the 2017 ACM Asia Conference on Computer and Communications Security, Abu Dhabi, UAE. – 2017. – pp. 506–519.

8. Huang N. E. The Hilbert-Huang transform and its applications / Ed. By S.S. Shen. Interdisciplinary mathematical sciences. 5 Toh Tuck Link, Singapore 596224: World Scientific Publishing Company Co. Pte. Ltd., 2005. – 311 p.

9. Kaslovsky D. N., Meyer F. G. Noise corruption of Empirical Mode Decomposition and its effect on Instantaneous Frequency. Advances in Adaptive Data Analysis. – 2010. – Vol. 2. – No. 3. – P. 373–396.

10. Yeh J.-R., Shieh J.-S., Huang N. E. Complementary Ensemble Empirical Mode Decomposition: A Novel Noise Enhanced Data Analysis Method. Advances in Adaptive Data Analysis. – 2010. – Vol. 2. – No. 2. – P. 135–156.

11. Eftekhar, A., Toumazou, C. & Drakakis, E.M. J Sign Process Syst. – 2013. – Vol. 73. – No. 43. DOI: 10.1007/s11265-012-0726-y

12. Сафиуллин Н. Т. Повышение быстродействия ансамблевой эмпирической модовой декомпозиции распараллеливанием алгоритма // 26-я Международная Крымская конференция «СВЧ-техника и телекоммуникационные технологии». КрыМиКо'2016. – Севастополь, 2016. – С. 593–599.

References

1. Shari Trewin, etc. Biometric authentication on a mobile device: a study of user effort, error and task disruption. In Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC '12). ACM, New York, NY, USA, – 2012. – pp. 159-168. DOI:10.1145/2420950.2420976

2. Alisa Kongthon, etc. Implementing an online help desk system based on conversational agent. In Proceedings of the International Conference on Management of Emergent Digital EcoSystems (MEDES '09). ACM, New York, NY, USA, – No. 69, – 2009. DOI:10.1145/1643823.1643908

3. Russian newspaper. Federal Issue No. 7515 (52). URL: https://rg.ru/2018/03/13/rossiiane-smogut-brat-kredity-i-otkryvat-vklady-po-vneshnosti-i-golosu.html (accessed on 28.03.2018)

4. Sergienko A. B. Digital signal processing. – 2nd. Ed. – 2007. – 751 p.

5. Tur, G., De Mori R., Spoken Language Understanding: Systems for Extracting Semantic Information from Speech. – John Wiley & Sons, Ltd – 23 March 2011. – 450 p. DOI: 10.1002/9781119992691

6. M. Hagan, H. Demuth, M. Beale. Neural Network Design. – Amazon Publ. 2nd ed. – 2016. – 1012 p.

7. Nicolas Papernot, Patrick McDaniel, Ian Goodfellow, Somesh Jha, Z. Berkay Celik, Ananthram Swami. Practical Black-Box Attacks against Machine Learning. Proceedings of the 2017 ACM Asia Conference on Computer and Communications Security, Abu Dhabi, UAE. – 2017. – pp. 506-519.

8. Huang N. E. The Hilbert-Huang transform and its applications / Ed. By S.S. Shen. Interdisciplinary mathematical sciences. 5 Toh Tuck Link, Singapore 596224: World Scientific Publishing Company Co. Pte. Ltd., 2005. – 311 p.

9. Kaslovsky D. N., Meyer F. G. Noise corruption of Empirical Mode Decomposition and its effect on Instantaneous Frequency. Advances in Adaptive Data Analysis. – 2010. – Vol. 2. – No. 3. – P. 373–396.

10. Yeh J.-R., Shieh J.-S., Huang N. E. Complementary Ensemble Empirical Mode Decomposition: A Novel Noise Enhanced Data Analysis Method. Advances in Adaptive Data Analysis. – 2010. – Vol. 2. – No. 2. – P. 135–156.

11. Eftekhar, A., Toumazou, C. & Drakakis, E.M. J Sign Process Syst. – 2013. – Vol. 73. – No. 43. DOI: 10.1007/s11265-012-0726-y

12. Safiullin N.T. Povishenie bistrodeystvia ansamblevoi empiricheskoi modovoi decomposicii rasparallelivaniem algoritma // 26th Mezdunarodnaya Crimskaya conference «SVCH-tehnika & telecommunicationnie tehnologii». Crimico 2016. – Sevastopol, 2016. – 593-599 p.

ДРЕСВЯНИН Павел Дмитриевич, студент магистратуры Института Радиоэлектроники и Информационных Технологий Уральского Федерального Университета им. Первого Президента России Б.Н. Ельцина. 620002 г. Екатеринбург, ул. Мира, 32. E-mail: pdresvyanin@bk.ru

САФИУЛЛИН Николай Тахирович, канд. техн. наук, доцент Департамента Информационных Технологий и Автоматики, Института Радиоэлектроники и Информационных Технологий Уральского Федерального Университета им. Первого Президента России Б.Н. Ельцина. 620002 г. Екатеринбург, ул. Мира, 32. E-mail: n.t.safiullin@urfu.ru

ПОРШНЕВ Сергей Владимирович, докт. техн. наук, проф., директор Учебно-научного центра «Информационная безопасность» Института Радиоэлектроники и Информационных Технологий Уральского Федерального Университета им. Первого Президента России Б.Н. Ельцина. 620002 г. Екатеринбург, ул. Мира, 32. E-mail: s.v.porshnev@urfu.ru

DRESVYANIN Pavel, student of Institute of Radioelectronics and Information Technologies of Ural Federal University. 620002, Russia, Yekaterinburg, 32 Mira Street. E-mail: pdresvyanin@bk.ru

SAFIULLIN Nikolai, Candidate of Technical Sciences, Docent of Department of Information Technologies and Automation, Institute of Radioelectronics and Information Technologies of Ural Federal University. 620002, Russia, Yekaterinburg, 32 Mira Street. E-mail: n.t.safiullin@urfu.ru

PORSHNEV Sergey, Doctor of Technical Sciences, Professor, Director of Scientific-Educational Center for «Information Security», Institute of Radioelectronics and Information Technologies of Ural Federal University. 620002, Russia, Yekaterinburg, 32 Mira Street. E-mail: s.v.porshnev@urfu.ru

УДК 004.056:343.98 + 343.983.25:004.056 Вестник УрФО № 1(27) / 2018, с. 42–46

Зулькарнеев И. Р., Карпов М. Г., Нестор В. О., Семенов Д. Ю.

КОНЦЕПЦИЯ СОЗДАНИЯ КРИМИНАЛИСТИЧЕСКОГО ДУБЛИКАТОРА ДАННЫХ

В данной статье авторами поднимается вопрос о возможности и целесообразности реализации аппаратного дубликатора данных пригодного для проведения криминалистических экспертиз. Определены основные проблемы реализации аппаратного дубликатора и методы их решения. Проведен сравнительный анализ программируемых микроконтроллеров по заявленным критериям. Сделан вывод о возможности и необходимости создания подобного дубликатора.

Ключевые слова: *компьютерно-техническая экспертиза, форензика, микроконтроллеры, дубликаторы, блокираторы записи.*

Zulkarneev I. R., Karpov M. G., Nestor V. O., Semenov D. Y.

THE CONCEPT OF CRIMINALISTIC DATA DUPLICATOR DEVELOPING

The article considers the issues of possibility and feasibility of hardware data duplicator developing in computer forensics. It is defined the main problems of hardware duplicator creation and the methods of solving these problems. The comparative analysis of software microcontrollers was done by the declared criterias. It is concluded that hardware duplicator developing is possible and necessary.

Keywords: *computer forensics, microcontrollers, duplicators, write blocker*

При производстве компьютерно-технической экспертизы (КТЭ) необходимо следовать юридически закрепленным требованиям, регламентирующим данную деятельность. Одно из таких требований – обеспечение неизменности, сохранности объектов исследования [1].

В рамках КТЭ выделяют следующие группы объектов: аппаратные, программные, информационные, сетевые. Все перечисленные группы ориентированы на различные подходы к исследованию центрального объекта КТЭ – информации (данных). Принимая во внимание факт того, что информация хранится на различных типах устройств, необходимо конкретизировать область данного исследования. Самыми распространенными носителями информации, которые предоставляется эксперту, являются электронные накопители данных, в частности постоянные запоминающие устройства [2]. На текущий момент на отечественном рынке не существует надежного

способа сохранения целостности данных, использующих флеш-память. Как следствие, в данной статье под объектами исследования КТЭ будут пониматься накопители на жестких магнитных дисках (НЖМД).

Обеспечение целостности объектов исследования позволяет в рамках КТЭ реализовать:

- проведение повторной или дополнительной экспертизы, так как при нарушении целостности доказательства повторная экспертиза может дать отличное от предыдущего заключение;
- обеспечение сохранности улик, с целью исключения внесения изменений, в том числе непреднамеренных и срабатывания логических бомб на исследуемых объектах;
- обеспечение беспристрастности эксперта, ввиду невозможности его влияния на предоставленные для экспертизы материалы дела.

В случае внесения каких-либо изменений в вещественные доказательства без предварительного уведомления заказчика заключение эксперта признается недействительным, а само доказательство исключается из материалов дела. Все это позволяет говорить о необходимости обеспечения целостности объектов исследования, как об основном требовании проведения корректной и легальной компьютерно-технической экспертизы.

Обеспечить выполнение требования целостности данных возможно с использованием следующих методов, имеющих как программную, так и аппаратную реализацию: исследование устройства с применением блокиратора записи и создание копии данных исследуемого устройства [3].

Рассмотрим метод блокирования записи. Взаимодействии с НЖМД осуществляется с помощью команд группы «read», считывающих данные с диска, и команд группы «write», записывающих данные и вносящих какие-либо изменения на диск. Блокираторы записи позволяют производить исследование непосредственно на НЖМД, предотвращая реализацию команд группы «write». Это позволяет повысить скорость исследования (так как нет необходимости затрачивать время на создание дубликата НЖМД), а также производить необходимые действия без использования дополнительных накопителей (таким образом можно исследовать устройство любого объема). На рис. 1 представлена общая схема работы такого метода: блокиратор обрабатывает все операции между накопителем и ПК, кроме команд группы «write».

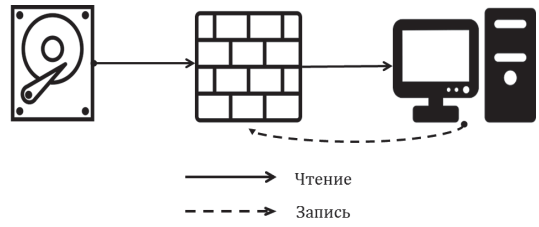


Рис. 1. Общая схема работы блокиратора записи

Программная реализация блокираторов записи может существовать как на уровне драйвера ядра операционной системы, так и в виде высокоуровневого драйвера фильтров. В первом случае, драйвер перехватывает любое обращение к устройству на низком уровне, блокируя посылаемые сигналы. Во втором случае, блокиратор также перехватывает запросы к драйверу устройства и фильтрует команды на запись, выполняя операции на высоком уровне.

Аппаратные блокираторы записи имеют две реализации: работающие в качестве транслятора и в качестве посредника команд. Блокираторы, работающие по принципу транслятора, получая команду, сверяют ее со списком разрешенных (или запрещенных) команд и далее, если было найдено совпадение, повторяют ее для целевого устройства (или отклоняют). Блокираторы, работающие в качестве посредника, представляют собой миникомпьютер со встроенной программной реализацией блокиратора, и, как следствие имеют операционную систему. Аппаратные блокираторы записи, не имеющие операционной системы, по сравнению с программными блокираторами являются более надежными, потому что спроектированы так, что в случае возникновения ошибок не смогут физически осуществить запись на НЖМД [4].

Метод дублирования данных позволяет не беспокоится о целостности исследуемого объекта во время проведения КТЭ, так как все данные предварительно копируются на сторонний накопитель, с которым и будет взаимодействовать эксперт. Дубликатор данных, создавая полную посекторную копию исследуемого накопителя, оперирует командами прошивки накопителя с последующей обработкой информации (вычисление контрольных сумм, для последующей валидации копии).

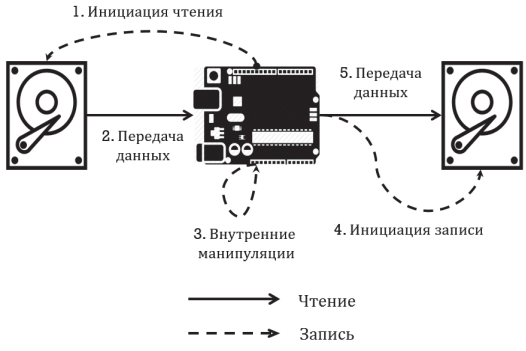


Рис. 2. Общая схема работа дубликаторов данных

Программная реализация дубликаторов функционирует на основе операционной системы, поэтому скорость копирования может быть ниже в сравнении с аппаратными реализациями, так как для взаимодействия с НЖМД программе необходимо обратиться к операционной системе, что влечет за собой лишние системные вызовы. На ОС запущено множество других процессов, которые занимают процессорное время, что также затормаживает копирование. Из недостатков данного подхода можно отметить, что подобная реализация, как правило, обладает недекларированными возможностями, следовательно есть вероятность испортить исследуемый объект при создании копии, повредив его целостность.

Аппаратные дубликаторы данных представлены в виде специального устройства, и в сравнении с их программными аналогами имеют значительно более высокие скорости копирования данных, так как взаимодействие программы с НЖМД осуществляется без операционной системы. Отсутствие ОС а также архитектура устройства (отсутствует канал «write» на аппаратном уровне) гарантирует, что дубликатор не нарушит целостности объекта исследования.

Обе реализации дубликаторов поддерживают два вида копирования данных: диск-диск и диск-образ. Первый способ производит полное посекторное копирование жесткого диска, итогом которого является новый НЖМД с аналогичными объемом и информацией. Второй способ «диск-образ» выполняет создание посекторной копии с преобразованием информации (сжатием). Итогом такого копирования является файл.

Стоит отметить, что существующие на рынке дубликаторы имеют зарубежное происхождение, а их стоимость высока для некрупных негосударственных экспертных учреждений. В связи с этим встает вопрос об исследовании возможности создания аппаратного дубликатора, который бы имел низкую себестоимость и реализовывал следующие функциональные возможности [5]:

реализация механизма создания копии НЖМД без возможности записи на оригинальный НЖМД на физическом уровне (криминалистически верная копия);

- генерация и валидация контрольных-сумм секторов НЖМД;
- журналирование событий.

Одна из проблем стоящих при создании дубликатора данных – это выбор программируемого микроконтроллера (ПМ). Для достижения целей исследования требуется оценка ПМ по следующим критериям:

- объем оперативной памяти – для обеспечения максимально возможной скорости копирования
- тактовая частота процессора;
- возможность работы без операционной системы;
- средняя стоимость.

Основным критерием является возможность работы без операционной системы для уменьшения вероятности сбоя блокировки записи при копировании НЖМД. В связи с этим в сравнении микроконтроллеров не участвовал Raspberry Pi. Для сравнения авторами были выбраны наиболее популярные и доступные ПМ: STM32F4, Teensy 3.6, Arduino Uno. Результаты отражены в таблице.

Характеристики программируемых микроконтроллеров

Характеристики	STM32F4 Discovery	Teensy 3.6	Arduino Uno
Тактовая частота процессора	168 МГц	180 МГц	16 МГц
Объем оперативной памяти	192 кБ	256 Кб	2 Кб
Возможность работы без ОС	Да	Да	Да
Средняя стоимость	1700	2 070	520

С учетом заявленных требований наиболее подходящим ПМ является Teensy 3.6.

При решении поставленной задачи может возникнуть проблема чтения поврежденных секторов. Предустановленное системное программное обеспечение на НЖМД, возвращает сообщение об ошибке в случае, если

значение бита достоверно неизвестно, следовательно, при считывании диск не сможет вернуть информацию с НЖМД. В качестве решения данной проблемы предполагается использование команды Read Long, благодаря которой верификация возвращаемой информации не осуществляется, а происходит считывание поврежденного сектора определенное количества раз и выбор наиболее часто встречающегося значения [6]. Данная команда поддерживается большинством современных НЖМД.

Разница в объемах целевого и исходного НЖМД также является проблемой, на которую следует обратить внимание. Для ее решения следует делать проверку, перед копированием данных. Если объем исходного диска больше объема целевого, то требуется выводить сообщение об ошибке, иначе необходимо установить HPA (Host Protected Area) равной разнице объемов на целевом жестком диске и начать копирование.

Помимо выше изложенных проблем необходимо принимать во внимание и другие неустранимые факторы, которые могут приводить к искажению информации в процессе ее передачи и записи. С целью контроля таких искажений следует использовать механизм проверки целостности, основанный на контрольных суммах. При этом для эффективного детектирования искаженных битов оптимально вычислять контрольную сумму от каждого сектора НЖМД, а не общую ото всех секторов. Последняя проблема, которую предстоит решить – это самодостаточность и простота дубликатора. Устройство должно быть независимым от других устройств, а именно: снабжать питанием подключенные НЖМД, журналировать события и копировать данные самостоятельно. Следовательно, предположительная модель устройства должна выглядеть следующим образом: к дубликатору будут подключатся исходный и целевой НЖМД, информация с исходного будет проходить через дубликатор, где будет производится проверка на возможные ошибки считывания, на целевой НЖМД. Схема работы дубликатора представлена на рис. 3.

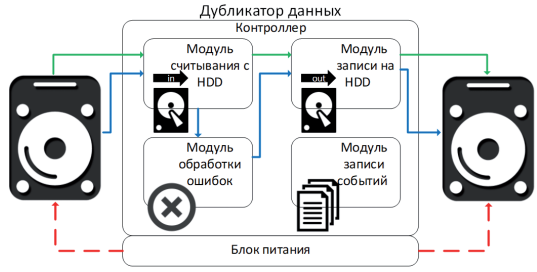


Рис. 3. Принципиальная схема дубликатора

Исходя из полученных данных можно сделать однозначный вывод о возможности и целесообразности создания аппаратного дубликатора на основе программируемого микроконтроллера с заявленным функционалом для небольших негосударственных экспертных учреждений. Коллектив авторов считает необходимым дальнейшее исследование данного вопроса и разработку прототипа дубликатора.

Литература

1. Федеральный закон от 31.05.2001 № 73-ФЗ (ред. от 08.03.2015) "О государственной судебно-экспертной деятельности в Российской Федерации». – URL: http://www.consultant.ru/document/cons_doc_LAW_31871(дата обращения: 19.12.2017)

2. А. А. Шулепанов, А. Р. Смолина. Методика проведения подготовительной стадии исследования при производстве компьютерно-технической экспертизы. // Доклады Томского государственного университета систем управления и радиоэлектроники. Том 19 № 1. С. 31–34.

3. Mark Menz, Steve Bress. The Fallacy of Software Write Protection in Computer Forensics // MyKey Technology Inc. URL: http://mykeytech.com/softwarewriteblocking2-4.pdf (дата обращения: 15.11.2017)

4. ГОСТ Р ИСО/МЭК 27037-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме.

5. Сергей Прокопенко. Проблемы копирования данных с накопителей с дефектными секторами при производстве компьютерно-технических экспертиз // Лаборатория компьютерной криминалистики ЕПОС. URL: http://www.epos.ua/cp/pf/publications/data/upimages/imaging-bad-sectors-computer-forensics_prokopenko.pdf (дата обращения: 15.11.2017)

6. Берд Киви. Закон Мерфи для хранения данных // Цифровой журнал «Компьютерра» № 58 [28.02.2011 — 06.03.2011] URL: http://old.computerra.ru/own/kiwi/597770/

References

1. Federal'nyj zakon ot 31.05.2001 № 73-FZ (red. ot 08.03.2015) "O gosudarstvennoj sudebno-jekspertnoj dejatel'nosti v Rossijskoj Federacii" URL: http://www.consultant.ru/document/cons_doc_LAW_31871 (data obrashhenija: 19.12.2017)

2. Shulepanov, A. R. Smolina. Metodika provedenija podgotovitel'noj stadii issledovanija pri proizvodstve komp'juterno-tehnicheskoj jekspertizy. // Doklady Tomskogo gosudarstvennogo universiteta sistem upravlenija i radiojelektroniki. Tom 19 № 1. S. 31–34.

3. Mark Menz, Steve Bress. The Fallacy of Software Write Protection in Computer Forensics // MyKey Technology Inc. URL: http://mykeytech.com/softwarewriteblocking2-4.pdf (data obrashhenija: 15.11.2017)

4. GOST R ISO/MJeK 27037-2014. Informacionnaja tehnologija. Metody i sredstva obespechenija bezopasnosti. Rukovodstva po identifikacii, sboru, polucheniju i hraneniju svidetel'stv, predstavlennyh v cifrovoj forme.

5. Sergej Prokopenko. Problemy kopirovanija dannyh s nakopitelej s defektnymi sektorami pri proizvodstve komp'juterno-tehnicheskih jekspertiz // Laboratorija komp'juternoj kriminalistiki EPOS. URL: http://www.epos.ua/cp/pf/publications/data/upimages/imaging-bad-sectors-computer-forensics_prokopenko.pdf (data obrashhenija: 15.11.2017)

6. Berd Kivi. Zakon Mjorfi dlja hranenija dannyh // Cifrovoj zhurnal «Komp'juterra» № 58 [28.02.2011 — 06.03.2011] URL: http://old.computerra.ru/own/kiwi/597770/

ЗУЛЬКАРНЕЕВ Искандер Рашитович, старший преподаватель кафедры информационной безопасности Института математики и компьютерных наук ТюмГУ. 625003, г. Тюмень, ул. Володарского, д. 6. E-mail: i.r.zulkarneev@utmn.ru

КАРПОВ Михаил Георгиевич, студент 4 курса направления «Информационная безопасность» Института математики и компьютерных наук ТюмГУ. 625003, г. Тюмень, ул. Володарского, д. 6. E-mail: m.g.karpov@utmn.ru

НЕСТОР Владимир Олегович, студент 3 курса направления «Компьютерная безопасность» Института математики и компьютерных наук ТюмГУ. 625003, г. Тюмень, ул. Володарского, д. 6. E-mail: r3seh@ya.ru

СЕМЕНОВ Дмитрий Юрьевич, студент 4 курса направления «Информационная безопасность» Института математики и компьютерных наук ТюмГУ. 625003, г. Тюмень, ул. Володарского, д. 6. E-mail: sdu9692@gmail.com

ZULKARNEEV Iskander, Senior Lecturer, Information Security Department, Institute of Mathematics and Computer Science, Tyumen State University6 Volodarskogo St., 625003 Tyumen, Russia. E-mail: i.r.zulkarneev@utmn.ru

KARPOV Mikhail, student of the 4th year of the course "Information Security" of the Institute of Mathematics and Computer Science of Tyumen State University. 6 Volodarskogo St., 625003 Tyumen, Russia. E-mail: m.g.karpov@utmn.ru

NESTOR Vladimir, student of the 3rd year of the course "Computer Security" of the Institute of Mathematics and Computer Science of Tyumen State University. 6 Volodarskogo St., 625003 Tyumen, Russia. E-mail: r3seh@ya.ru

SEMENOV Dmitry, student of the 4th year of the course "Information Security" of the Institute of Mathematics and Computer Science of Tyumen State University. 6 Volodarskogo St., 625003 Tyumen, Russia. E-mail: sdu9692@gmail.com

УДК 004.056 Вестник УрФО № 1(27) / 2018, с. 47–56

Семенищев И. А., Синадский А. Н., Синадский Н. И., Сушков П. В.

СИНТЕЗ МАССИВОВ БИЛЛИНГОВОЙ ИНФОРМАЦИИ НА ОСНОВЕ СТАТИСТИКО-СОБЫТИЙНОЙ МОДЕЛИ ВЗАИМОДЕЙСТВИЯ АБОНЕНТОВ СЕТЕЙ СОТОВОЙ СВЯЗИ

В статье рассмотрен программный комплекс, реализующий алгоритм синтеза массивов биллинговой информации на основе разработанной пространственно-временной статистико-событийной модели, приводятся статистические характеристики синтезируемых массивов и результаты их обработки; комплекс предназначен для тестирования информационно-аналитических систем безопасности и обеспечения практических занятий по дисциплинам направления «Информационная безопасность».

Ключевые слова: *синтез массивов биллинговой информации, информационно-аналитические системы безопасности.*

Semenishchev I. A., Sinadsky A. N., Sinadsky N. I., Sushkov P. V.

SYNTHESIS BILLING INFORMATION ARRAYS BASED ON THE STATISTICAL EVENT MODEL OF INTERACTION OF CELLULAR NETWORKS SUBSCRIBERS

The article introduces the software complex that implements the algorithm for synthesizing an array of billing information based on a spatio-temporal statistical-event model, statistical characteristics of synthesized arrays and the results of their processing. The complex is designed for testing information and analytical security systems and providing practical classes in the disciplines of the specialty Information Security.

Keywords*: Synthesis of arrays of billing information, information-analytical security systems.*

Вступление в силу Федерального закона 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» свидетельствует об актуальности и значимости разработки программно-аппаратных систем, предназначенных для решения задач по обнаружению, предупреждению и ликвидации последствий компьютерных атак на критическую информационную инфраструктуру (КИИ) Российской Федерации. Задачи обнаружения компьютерных атак и расследования компьютерных инцидентов решаются, в том числе информационно-аналитическими системами безопасности (ИАСБ), одним из примеров которых является система DATAPK [1], представляющая собой комплекс оперативного мониторинга и контроля защищенности объектов КИИ.

В рамках обеспечения информационной безопасности на каналах сотовой связи применяются и активно разрабатываются поисково-аналитические системы, такие как IBM I2[1], МФИ СОФТ «Январь»[2] и др., использующие сложные алгоритмы поиска взаимосвязей элементов современных телекоммуникационных систем. Эти программы применяются службами информационной безопасности операторов сетей сотовой связи с целью выявления, в том числе, фактов мошенничества при оплате услуг.

Для тестирования корректности реализации аналитических алгоритмов в системах различного типа требуются массивы биллинговой информации. Аналогичные массивы должны использоваться для обеспечения образовательного процесса в рамках изучения ИАСБ как на потоках магистратуры по направлению «Информационная безопасность», так и на потоках специалитета «Информационная безопасность телекоммуникационных систем» и «Информационно-аналитические системы безопасности».

При этом использование настоящих массивов биллинговой информации о взаимодействии абонентов сетей сотовой связи невозможно, в том числе в силу ограничений, накладываемых ФЗ «О связи». Кроме того, для анализа алгоритмов ИАСБ необходим эталонный трафик, статистические распределения, характер связей элементов и конкретные связи между заданными элементами которого должны быть точно известны.

Целью работы является разработка программного обеспечения для синтеза массивов биллинговой информации, состоящих из фонового биллинга, являющегося информационным наполнением, на которое накладывается массив ситуационных задач (тестов), с целью формирования у студентов практических навыков по поиску и анализу взаимосвязей элементов современных телекоммуникационных систем.

Создан программный комплекс, позволяющий осуществлять синтез массивов биллинговой информации и массивов данных, имитирующих взаимодействие пользователей в социальных сетях. В основе комплекса лежит разработанная авторами пространственно-временная статистико-событийная модель взаимодействия пользователей в сетях операторов связи [2–5].

Программная реализация предложенной модели позволяет синтезировать массив биллинговой информации по заранее заданным статистическим распределениям и создавать требуемые связи между элементами сети.

Вариативность статистических распределений, описывающих характеристики фонового массива биллинга, позволяет создавать тестовые массивы как общего вида, так и для конкретной ситуационной задачи, использующейся для постановки поисково-аналитических задач при изучении ИАСБ.

Структура массива биллинговой информации

Массив биллинговой информации представляет собой упорядоченную по временной метке совокупность записей. Каждая запись (строка) является структурой данных, в которую входят 12 полей, которые могут быть как заполненными, так и пустыми. Основными значимыми для генерации полями являются: AbonentIMSI (номер SIM-карты абонента), AbonentIMEI (тип и серийный номер устройства абонента), AbonentPhone (MSISDN – номер телефона), LAC и CellID (поля, указывающие на привязку к базовой станции), BillTime (время события), CallDuration (продолжительность соединения) и BillingType (тип события) (рис. 1).

BillTime	CallDuration	BillingType	LAC	CellID	PhoneB	AbonentIMEI	AbonentIMSI	AbonentPhone
06.06.2014 0:00	4	Normal LocUpd	3901	39762		357331049414210	250023622333809	79222244716
06.06.2014 0:00	3	GPRS	3901	39762		353160046567420	250280422334339	79052245247
06.06.2014 0:00	4	GPRS	3907	39781		357881046123760	250027122338724	79322249642
06.06.2014 0:00	1	SMS In	3907	3024	79222241006	12536006306700	250011422337848	79822248766
06.06.2014 0:00	4	SMS In	3907	3024	79122253586	357008045261270	250011522326032	79122236947
06.06.2014 0:00	4	GPRS	3901	39762		359290056323320	250284722325348	79052236267
06.06.2014 0:00	4	Normal LocUpd	3907	3024		357881045550410	250027022325792	79222236705
06.06.2014 0:00	2	Normal LocUpd	3907	39781		357331049962830	250023622326087	79222237008
06.06.2014 0:00	0	SMS Out	3901	39762	7922256258	357881043528250	250027122345377	79222256280

Рис. 1. Строки массива биллинговой информации

[1] http://www-03.ibm.com/software/ products/ru/analysts-notebook

[2] http://www.mfisoft.ru/direction/sorm/sorm-3/

Под термином «абонент» понимается элемент сети (узел графа) сотовой связи, инициирующий или принимающий соединения. Соединение –– это направленная ветвь от одного узла графа к другому. Инициатором соединения называется исходный для этой ветви узел, принимающим абонентом – конечный.

Массив биллинга формируется для коммутатора, принадлежащего одному из операторов сетей сотовой связи, и представляет собой совокупность записей, поступающих с различных базовых станций о совершаемых абонентскими устройствами действиях.

Пространственно-временная статистико-событийная модель биллинговой информации

Разработанный программный комплекс позволяет на основе имеющихся статистических распределений генерировать массивы биллинговой информации.

С целью синтеза массивов биллинговой информации предложена модель жителей населенного пункта в терминах телекоммуникаций [2]. В качестве основы модели выбрана популяция абонентов операторов сетей сотовой связи, проживающих на вымышленной территории, перемещающихся по заданным правилам в течение генерируемого периода времени и осуществляющих взаимодействие путем совершения звонков и отправки СМС (SMS)-сообщений в соответствии с задаваемыми статистическими распределениями.

Пространственно-временная статистико-событийная модель *M* синтеза биллинговой информации, основанная на поведении абонентов с точки зрения сети операторов связи, является совокупностью модели перемещений абонентов в течение заданного промежутка времени *MSH*, модели соединений *MS* и модели *MTG* отправки сообщений о подключениях к базовым станциям для передачи координат и получения GPRS-трафика.

На данном этапе разработки предполагается, что один типовой абонент имеет один телефонный аппарат (IMEI) и одну идентифицирующую его SIM-карту (IMSI). Генерируются только значимые для последующего анализа события: служебные записи, не влияющие на анализ, при генерации игнорируются.

Модель соединений *MS* учитывает статистические распределения биллинговой информации и социальные характеристики абонентов операторов сотовой связи (круг общения: наличие родственных, личных связей). Социальные характеристики представлены шаблонами поведения для различных социальных групп, включая характеристики взаимодействия в сетях сотовой связи и характеристики перемещения людей в рамках населенного пункта.

В состав модели соединений *MS* вводятся множества абонентов оператора сотовой связи *H*: $H = \{h_i\}_{i=1}^{n_h}$ и «семей» *W*: $W = \{w_i \mid w_i \subseteq H\}_{i=1}^{n_w}$, n_h – количество абонентов, n_w – «семей».

Абонентские терминалы представлены в модели множествами номеров IMSI, IMEI и MSISDN с количеством элементов, равным n_h: $N_{imsi} = \{n_{imsi_i}\}_{i=1}^{n_h}$, $N_{imei} = \{n_{imei_i}\}_{i=1}^{n_h}$, $N_{msisdn} = \{n_{msisdn_i}\}_{i=1}^{n_h}$. Для формирования элементов множеств используется алгоритм генерации неповторяющихся чисел требуемого формата.

Совокупность абонентов и соответствующих им абонентских терминалов формирует абонентскую базу (базу принадлежности).

Модель перемещений *MSH* предназначена для генерации полей, описывающих географические координаты совершения события, имитирует перемещения абонентов в заданном временном интервале в рамках населенного пункта, который представляется квадратом, состоящим из массива клеток (рис. 2). Для каждой клетки задаются модифицируемые списками параметры LAC (Location Area Code – код локальной зоны) и CellID (уникальный номер, предназначенный для идентификации базовых станций).

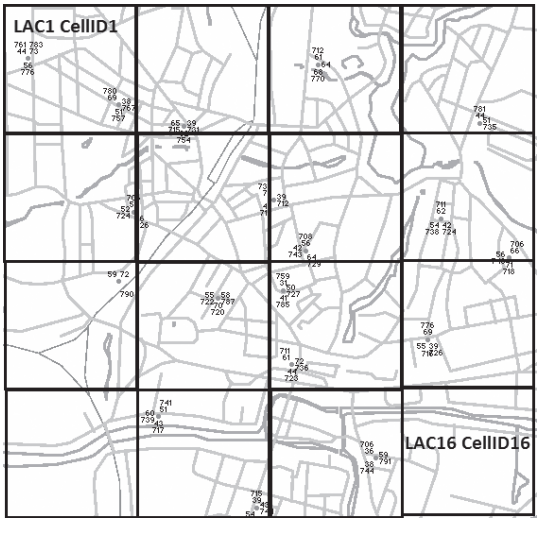


Рис. 2. Схема разделения моделируемой территории на области действия базовых станций

Перемещения абонентов могут моделироваться в двух совмещаемых режимах: на основе частотных распределений по популярности конкретных зон или на основе шаблонов перемещений. В первом случае перемещения абонентов имеют большую случайность, возможность быстрого редактирования характера перемещений абонентов путем изменения приоритетов конкретных зон (ячеек карты), во втором перемещения предсказуемы и направляемы (пользователь может менять маршруты абонентов и указывать конкретные точки маршрута по своему усмотрению), что требуется при создании ситуационной задачи.

Передвижение абонентов в рамках населенного пункта описывается шаблонами перемещений *SH*. Количество шаблонов произвольное, задается значением n_{sh}, $SH = \{sh\}_{i=1}^{n_{sh}}$. Шаблон перемещений представляет собой упорядоченный по времени список LAC и CellID, по которому отслеживается передвижение абонента в течение заданного времени.

Населенный пункт характеризуется массивом ячеек его карты: двумерным вектором *map*, n_{map} – его длина (количество ячеек карты), в каждом $map \in \overline{(1, n_{map})}$ из элементов которого содержатся два параметра (LAC и CellID) базовой станции, обслуживающей участок территории.

При генерации массива абонентов *H* каждому абоненту h_i присваивается номер, соответствующий шаблону перемещений sh_i из массива шаблонов *SH*. Соответственно, каждому абоненту назначается начальная точка на карте и перечень точек его местонахождения в последующие моменты времени.

В синтезируемом массиве строк биллинга *D*: $D = \{d\}_{i=1}^{n_d}$ (n_d – количество строк) каждая строка соответствует событию (действию) в сети. Строки массива *D* формируются из массивов, описывающих события различного типа – *T, G, C* и *S*:

T – массив событий отправки сообщений о подключениях к базовым станциям для передачи координат: $T = \{t\}_{i=1}^{n_t}$;

G – массив событий получения GPRS-трафика: $G = \{g\}_{i=1}^{n_g}$;

C – массив звонков $C = \{c\}_{i=1}^{n_c}$, состоит из массивов исходящих C_o и входящих C_i звонков: $C = C_i + C_o$;

S – массив СМС-сообщений $S = \{s\}_{i=1}^{n_s}$, состоит из массивов исходящих S_o и входящих S_i СМС-сообщений: $S = S_i + S_o$ (где n_t – количество перемещений, n_g – подключений, n_c, n_{co} и n_{ci} – звонков, n_s, n_{si} и n_{so} – сообщений, причём $n_c = n_{ci} + n_{co}$, $n_s = n_{si} + n_{so}$).

Массив соединений *Y* является совокупностью массива звонков и массива СМС-сообщений: $Y = C + S$, где n_y – количество соединений ($n_y = n_c + n_s$). Характеристики элементов массива соединений *Y*:

– идентификатор типа соединения абонентов $\boldsymbol{A} \in \overline{(1, n_a)}$, n_a – количество различных типов соединений;

– идентификаторы абонентов, участвующих в соединении – абоненты $h_1, h_2 \in H$ – источник и получатель соединения;

– идентификаторы абонентов h_1 и h_2 в сети сотовой связи (IMSI, MSISDN, IMEI), где n_p – предельное значение параметра: $p_1,\ p_2 \in \overline{(1, n_p)}$.

При формировании массива соединений *Y* учитываются статистические характеристики биллинговой информации:

– $K_0 = \langle F_{time}, F_{dur}, F_n, F_a \rangle$ – не связанные с адресацией соединения, описываемые функциями распределения: F_{time} – времени суток, F_{dur} – длительности события, F_n – количества соединений, F_a – вероятности генерации типа события;

– $K_1 = \langle F_l, F_t \rangle$ – связанные с адресацией соединения: F_l – функция распределения выбора получателей соединения, а F_t – функция распределения промежутков времени между началами инициализации двух последовательных соединений.

Таким образом, структура соединений определена вектором $\langle Y_i \rangle_{i=1}^{n_Y}$ и описывается выражением: $Y_i = \langle A, h_1, h_2, p_1, p_2, K_0, K_1 \rangle$.

Модель соединений *MS* определяется выражением: $MS = \langle H, W, \langle Y_i \rangle_{i=1}^{n_Y} \rangle$.

Модель отправки сообщений о подключениях к базовым станциям для передачи координат и получения GPRS-трафика *MTG* формирует массивы *T* и *G* аналогично модели соединений, за исключением необходимости выбора получателя соединения (ввиду ненаправленности события) и совершения обратного соединения.

С учетом перемещений абонентов по заданным шаблонам пространственно-временная статистико-событийная модель *M* взаимодействия абонентов в сетях операторов сотовой связи описывается выражением: $M = \langle MS + MSH + MTG \rangle$.

На основе разработанной модели создан программный комплекс, решающий задачу синтеза массивов биллинговой информации, в котором для построения модели соедине-

ний *MS* на основе модели перемещений *MSH* использован алгоритм сетей Петри. Модель соединений *MS* (направленных событий) описывается в терминах сетей Петри, где в качестве множества узлов $P = \{p_i\}_{i=1}^{n_p}$ (n_p – количество) принимаются участвующие в соединениях абоненты, а в качестве индикатора наличия соединения между абонентами – вес связывающего перехода.

Каждый узел связан переходом с каждым: если $i \neq j$, то узлы p_i и p_j связаны переходом. Множество всех разрешенных (на которых имеется фишка) переходов сети $T = \left\{\{t_i\}_{j=1}^{n_{ti}}\right\}_{i=1}^{n_p}$ обозначим (n_{ti} – их количество на p_i, t_{ij} – j-й переход от узла p_i). Переход называется разрешенным, если его вес больше 0. Каждый переход t_{ij} обладает весом m(t_{ij}), имеющим смысл количества совершенных соединений между абонентами, которым соответствуют начальный $p_н$ и конечный $p_к$ узлы перехода. Количество элементов множества весов переходов графа равно количеству переходов $\sum_{i=1}^{n_p} n_{ti}$.

Множество всех разрешенных переходов сети обозначим $T_ш$, $n_{шti}$ – их количество на p_i, $t_{шij}$ – j-й переход от узла p_i, тогда $T_ш = \left\{\{t_{шi}\}_{j=1}^{n_{шti}}\right\}_{i=1}^{n_p}$.

Моделирование ситуации на основе заданного шаблона происходит в три этапа. На первом этапе из шаблона выделяются все n_p узлов, участвующих в соединениях, т. е. образуется множество $P = \{p_i\}_{i=1}^{n_p}$. После этого из шаблона выделяются все соединения между узлами и записываются в виде переходов, формируется множество $T_ш = \left\{\{t_{шi}\}_{j=1}^{n_{шti}}\right\}_{i=1}^{n_p}$.

Заметим, что в ходе построения модели ситуации множество узлов, описывающих ситуацию, может увеличиваться, но не может уменьшаться. В то же время количество переходов может как уменьшаться, так и увеличиваться.

На втором этапе сеть дополняется узлами и переходами, часть переходов запрещается или разрешается. Каждому узлу p_i случайно задается вес 0, 1 или 2. Условие y_k задания узлу конкретного значения веса зависит от полученного из шаблона количества разрешенных переходов с него $t_{шij}$. Условие y_{i1} задания узлу p_i веса 1 определяется по формуле

$$y_{i1} = \frac{n_{шti} - n_{шmin}}{n_{шmax} - n_{шmin}},$$

где, $n_{шmin} = min\left\{\left\{\{t_{шi}\}_{j=1}^{n_{шti}}\right\}_{i=1}^{n_p}\right\}$ т. е. минимальное количество разрешенных переходов из узла в шаблоне, а

$$n_{шmax} = max\left\{\left\{\{t_{шi}\}_{j=1}^{n_{шti}}\right\}_{i=1}^{n_p}\right\}$$

т. е. максимальное количество разрешенных переходов из узла в шаблоне. Условия y_{i0} задания узлу веса 0 и y_{i2} задания веса 2 определяются по формуле $y_{i0} = y_{i2} = \frac{1-y_{i1}}{2}$.

Узел p_j, получивший вес 0, удаляется. Для всех узлов $p_i \neq p_j$, не являющихся удаляемыми, выполняются следующие действия: в случае, если с узла p_i на удаленный узел p_j, и с узла p_j на узел $p_k \neq p_i$ переход был разрешен, то переход с узла p_i на узел p_k разрешается (вес увеличивается на 1). Если до этого действия переход узла p_i на узел p_k уже был разрешен, то к его весу прибавляется 1.

Узел, получивший вес 1, не изменяется. Переходы на него или с него могут изменяться лишь в том случае, если они изменяются вследствие изменения соседних (связанных с описываемыми разрешенными переходами) узлов.

Узел p_j, получивший вес 2, сохраняется. Кроме того, во множество P добавляется дополнительный узел p_k, связанный запрещенными переходами со всеми узлами из множества P, и только с узлом p_j – двумя разрешенными, причем один переход направлен от узла p_j к узлу p_k, а второй – в обратном направлении. После добавления узла p_k для него разрешаются переходы на такие p_i, переходы на которые с узла p_j являются разрешенными. Вес добавленного перехода с узла p_k на узел p_i равен весу перехода с узла p_j на узел p_i.

На третьем этапе всем разрешенным переходам задаются временные отметки в соответствии с распределением соединений по времени. При этом количество временных отметок, присваиваемых переходу, равно его весу.

После этого выполняется запись соединений, информация о которых хранится в сети Петри: последовательно для всех узлов из множества P строками в биллинге описываются их вес (количество строк), направленность (исходный узел – инициирующий абонент, конечный узел – принимающий абонент) и время (временная отметка в биллинге соответствует временному значению времени перехода, если значений времени перехода несколько, то для генерации каждой следующей строки они берутся последовательно).

Алгоритм формирования абонентской базы

Для генерации массива биллинговой информации необходимо иметь список абонентов, принимающих в нем участие. Для этого написана программа, генерирующая массив абонентов заданного размера.

На вход программе подаются списки фамилий, мужских и женских имен в порядке уменьшения статистической частоты появления в реальном мире, наборы 8-значных чисел, являющиеся 8 первыми цифрами IMEI сотовых телефонов и описывающими модель и происхождение телефона.

Описание каждого абонента хранится в отдельной строке. Каждый абонент имеет уникальный номер (от 0 до требуемого количества абонентов). Абоненты разделены по однопоколенным «семьям» – группам от 1 до 5 абонентов. Каждый абонент имеет «социальный статус» –– поле, содержащее двузначное число, цифра из разряда десятков которого обозначает количество «человек» в «семье» абонента, а вторая цифра –– «социальную роль» абонента (1 – отец, 2 – мать, 3, 4, 5 – дети).

Доля семей каждого типа (по количеству членов) в общем количестве генерируемых семей вычисляется, исходя из требуемого количества абонентов и распределения количества одиноких людей и реальных семей с различным количеством детей (0–3). Фамилия у всех членов семьи одна, отчество детей зависит от имени отца.

Каждому абоненту присваиваются номер оператора связи, которому он принадлежит, уникальные значения IMSI (номер SIM-карты), IMEI (номер аппарата) и MSISDN. Значения IMSI генерируется в зависимости от выбранного оператора связи, причем первому абоненту присваивается минимальное значение IMSI, а всем последующим –– следующее большее со случайным дискретом от 1 до 100. Значения IMEI генерируются случайно, первыми двумя цифрами могут быть 35 или 01, следующие 6 цифр –– номер модели, цифры с 9 по 14 –– серийный номер аппарата, генерируется аналогично IMSI. В значениях MSISDN первая цифра всегда 7 (Россия), от оператора связи зависят 3 цифры, остальные 7 цифр генерируются аналогично IMSI.

Алгоритм позволяет создавать до 100 миллионов уникальных номеров IMSI, IMEI и MSISDN.

Алгоритм и интерфейс программы для создания ситуационных задач

Для создания массива ситуационного биллинга оператору необходимо загрузить в приложение базу абонентов, в которой записаны их ФИО, IMSI, IMEI, MSISDN и т. д.

После загрузки базы в приложение появляется возможность сортировки базы и поиска абонента, который удовлетворяет критериям поиска: семейное положение и количество «человек» в «семье». Таким образом, оператор может выбрать несколько абонентов, которые в дальнейшем будут участниками ситуационного биллинга. Для абонентов в фоновом массиве биллинга задаются четыре типа событий (LocUpd, Call, SMS, GPRS). Все параметры соединений задаются в отдельной форме (рис. 3).

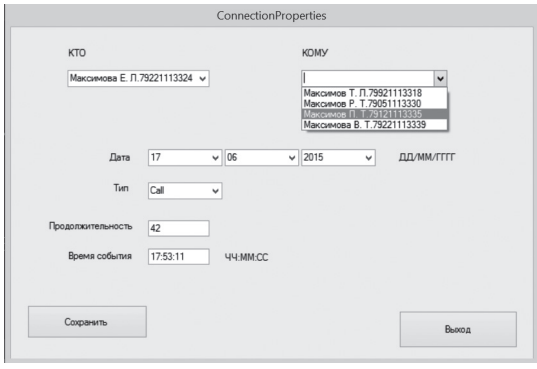


Рис. 3. Процесс добавления абонентов для формирования ситуационной задачи

В итоге в окне приложения (рис. 4) будет изображен граф, вершинами которого являются выбранные заранее абоненты, а ребрами –– настроенные соединения. После чего каждое соединение с учетом всех его параметров записывается в отдельный файл для каждого из коммутаторов, который описывает коммуникации группы людей за определенный период времени.

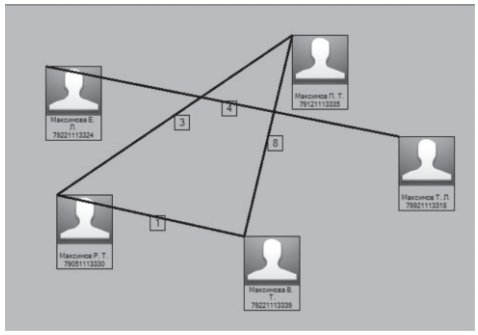


Рис. 4. Интерфейс модуля формирования ситуационной задачи

Считается, что одному оператору связи соответствует один коммутатор, при этом в стандартном населенном пункте присутствуют четыре основных оператора сотовой связи.

После генерации происходит встраивание массива ситуационного биллинга в фоновый.

Алгоритм синтеза фонового массива биллинговой информации

При синтезе фонового массива биллинговой информации используются абонентская база, созданная ранее, файл с LAC и CellID базовых станций выбранной местности, статистические распределения видов событий по времени и продолжительности, распределение количества звонков по дням недели, заранее сгенерированный массив ситуационного биллинга.

После выбора пользователем требуемого количества абонентов, участвующих в биллинге, часть абонентской базы записывается в оперативную память. Также из файлов считываются необходимые распределения и информация о расположении базовых станций, которая используется для создания «карты».

Перемещения генерируются в соответствии с заданными шаблонами. В шаблоне указывается соответствие часа суток и ячейки «карты», в которой находится абонент.

Затем происходит генерация «событий» – записей в массиве биллинга.

События генерируются поочередно для каждого из абонентов. Количество событий каждого вида, совершенных абонентом, выбирается по загруженным ранее статистическим распределениям.

Сначала по заданному в абонентской базе шаблону с использованием карты генерируются все перемещения, затем все GPRS-подключения.

После этого генерируются исходящие звонки. Их количество, продолжительность и время совершения события выбираются по загруженному ранее статистическому распределению. Абонент, которому направлен исходящий вызов, определяется следующим образом: с вероятностью, зависящей от количества «человек» в «семье» абонента и заданной ему при считывании абонентской базы количественной характеристики круга общения, происходит выбор одного из двух направлений соединения: абоненту из «семьи» или случайному. В случае звонка «семье» абонент гарантированно звонит «родственникам», в случае случайного собеседника – с вероятностью $P = \frac{\text{количество человек в семье} - 1}{\text{общее количество абонентов} - 1}$

«семье» и с вероятностью обратного события – иному абоненту.

После создания записи исходящего звонка от абонента А к абоненту В на коммутаторе абонента А создается запись входящего звонка для абонента В на коммутаторе абонента В. Этим достигается отсутствие необходимости отдельной генерации входящих звонков.

Исходящие и входящие СМС генерируются аналогично звонкам, отличие лишь в типе события и используемых распределениях.

После генерации всех событий для всех абонентов из базы принадлежностей, содержащей информацию об абонентах, в соответствующие массивы добавляются события, сгенерированные при создании ситуационной задачи, и начинается этап сортировки.

Сортировка выполняется для каждого коммутатора отдельно. Все (исходящие и входящие) события объединяются в единый массив. С целью оптимизации сортировки по времени создается дополнительный массив структур, состоящий только из двух полей: номера события (уникального для каждой записи) в исходном массиве и времени совершения события. После этого дополнительный массив сортируется по увеличению времени совершения события методом выбора. Затем информация из исходного массива в порядке номеров из дополнительного, уже отсортированного по времени, массива выводится в файл.

После повторения вышеописанных действий для каждого коммутатора массив биллинговой информации считается сформированным.

Статистические характеристики синтезируемых массивов

Для генерации фонового биллинга необходимы статистические распределения видов событий по времени и продолжительности, распределение количества звонков по дням недели и другие. Данные распределения были собраны на основе личного биллинга, обработаны и представлены в формате графиков.

Статистический анализ синтезируемого биллинга показывает, что его характеристики схожи с исходным массивом. В частности, распределение количества событий по дням недели демонстрирует всплеск активности в

пятничный вечер и падение на период выходных (рис. 5).

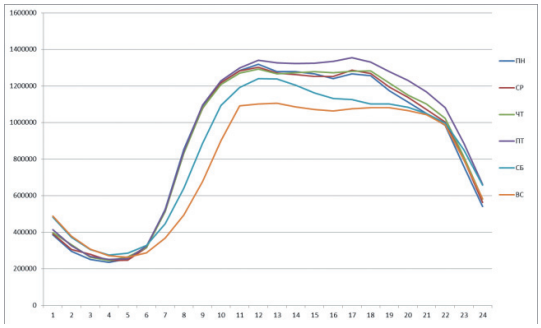


Рис. 5. Статистическое распределение объема биллинга по дням недели

Распределение по продолжительности звонков указывает на то, что большинство звонков длится менее 10 секунд (рис. 6).

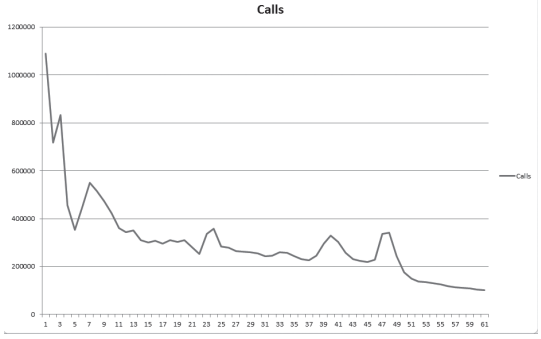


Рис. 6. График распределения продолжительности звонков

График распределения количества событий по времени суток в биллинге, сгенерированном для города с полуторамиллионным населением (рис. 7) показывает, что события обновления местоположения абонента (LocUpd) значительно превышают по количеству остальные типы событий (звонок, СМС-сообщение и подключение к GPRS).

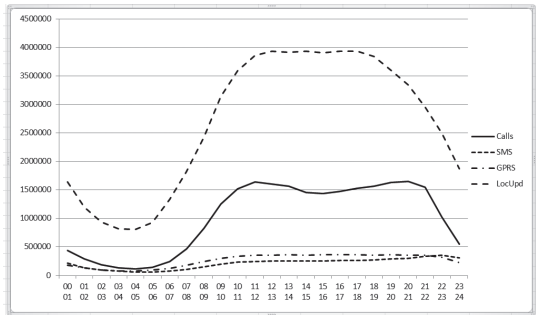


Рис. 7. График количественных отношений событий в биллинге в течение дня

Аналитические исследования [6] подтверждают корректность формируемых распределений. Таким образом, можно говорить о статистической схожести генерируемого биллинга и возможности его использования в практических приложениях.

Результаты обработки сформированного массива поисково-аналитическими комплексами

Для анализа сформированного массива возможно использовать программу IBM I2 или её аналог – открытую библиотеку CodePlex GraphSharp (рис. 8).

Программа адекватно воспринимает сформированный массив биллинга и предлагает несколько вариантов визуализации. При увеличении количества абонентов, участвующих в моделируемой сети, сложность взаимосвязей увеличивается.

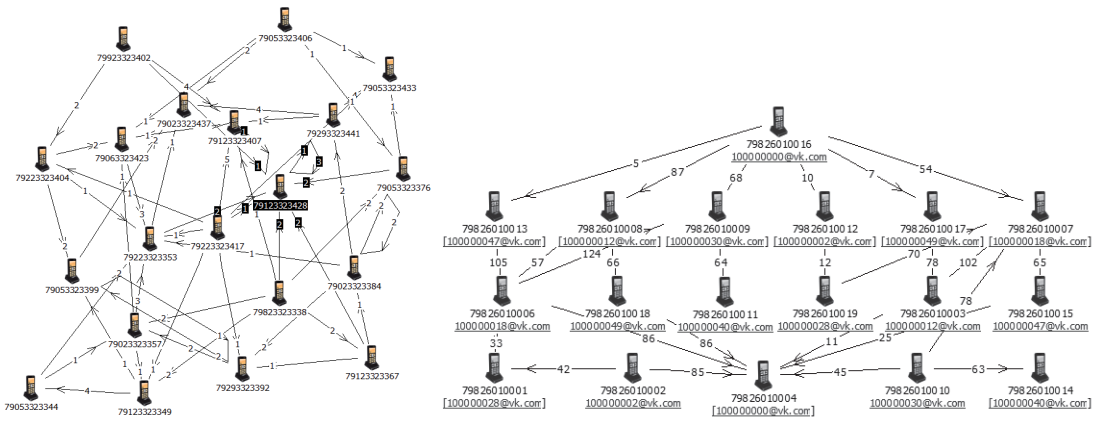


Рис. 8. Пример работы программы I2 при анализе сформированного биллинга на 20 абонентов

Структура и характеристики программного комплекса

Программный комплекс разработан на базе ОС Windows и состоит из программы генерации базы принадлежностей абонентов, программы создания ситуационных задач, программы статистического анализа массивов биллинговой информации и программы синтеза массивов биллинговой информации.

В процессе разработки программы синтеза массивов применен ряд оптимизационных решений по представлению данных в оперативной памяти и ускорению процессов сортировки записей по временным меткам. Для синтеза массивов биллинговой информации, описывающей взаимодействие 50 тысяч абонентов в течение 1 суток в вымышленном населенном пункте, где работают четыре оператора сотовой связи, при использовании одного стандартного персонального компьютера, оснащенного 8 ГБ оперативной памяти и процессором i7, требуется 1,5 часа. При этом в файлах биллинга формируется 30 миллионов строк, занимающих объем 2,7 Гб. Переносить информацию удобно в сжатом виде, тогда все файлы занимают не более 500 Мб. Формируемые объемы информации, а также время генерации являются приемлемыми для применения в образовательном процессе.

Выводы

Разработанный программный комплекс позволяет синтезировать массивы фонового биллинга, по статистическим характеристикам идентичные массивам биллинга реальных сетей операторов связи, и интегрировать в них ситуационные задачи, что дает возможность использовать данные массивы для тестирования поисково-аналитических систем и обеспечения практических занятий по изучению информационно-аналитических систем безопасности.

Литература

1. Программно-аппаратный комплекс DATAPK // DATAPK – комплекс оперативного мониторинга и контроля защищенности АСУ ТП. – URL: http://www.ussc.ru/catalog/id/74 (дата обращения: 05.03.2018).

2. Семенищев И. А., Синадский А. Н., Синадский Н. И. Алгоритм формирования массива биллинговой информации на основе статистической модели поведения абонентов сотовой связи // Сборник материалов XV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых «Безопасность информационного пространства». – Курган : Курганский ГУ, 2016. – С. 199–203.

3. Семенищев И. А., Синадский А. Н., Синадский Н. И. Статистические характеристики массива биллинговой информации при моделировании поведения абонентов сетей сотовой связи // Сборник материалов 12-ой международной молодежной научно-технической конференции «РТ–2016». – Севастополь : Севастопольский гос. ун-т, 2016. – С. 207.

4. Синадский А. Н., Синадский Н. И. Формальная математическая модель синтеза массива биллинговой информации // Сборник материалов XVI Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых «Безопасность информационного пространства». – Екатеринбург : УрФУ, 2017 (в печати).

5. Семенищев И. А., Синадский Н. И. Статистические характеристики синтезируемых массивов биллинговой информации // Сборник материалов XVI Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых «Безопасность информационного пространства». – Екатеринбург : УрФУ, 2017 (в печати).

6. Rao Zonghaoa, Yang Dongyuana, Duan Zhengyua. Resident Mobility Analysis Based on Mobile-Phone Billing Data // Procedia – Social and Behavioral Sciences, 96 (2013), С. 2032–2041.

References

1. Programmno-apparatnyy kompleks DATAPK // DATAPK – kompleks operativnogo monitoringa i kontrolya zashchishchennosti ASU TP. URL: http://www.ussc.ru/catalog/id/74 (data obrashcheniya: 05.03.2018).

2. Semenishchev I.A., Sinadskiy A.N., Sinadskiy N.I. Algoritm formirovaniya massiva billingovoy informatsii na osnove statisticheskoy modeli povedeniya abonentov sotovoy svyazi // Sbornik materialov XV Vserossiyskoy nauchno-prakticheskoy konferentsii studentov, aspirantov i molodykh uchenykh «Bezopasnost' informatsionnogo prostranstva». – Kurgan: Kurganskiy GU, 2016. – S. 199-203.

3. Semenishchev I.A., Sinadskiy A.N., Sinadskiy N.I. Statisticheskiye kharakteristiki massiva billingovoy informatsii pri modelirovanii povedeniya abonentov setey sotovoy svyazi // Sbornik materialov 12-oy mezhdunarodnoy molodezhnoy nauchno-tekhnicheskoy konferentsii «RT–2016». – Sevastopol', Sevastopol'skiy gosudarstvennyy universitet, 2016. – S. 207.

4. Sinadskiy A.N., Sinadskiy N.I. Formal'naya matematicheskaya model' sinteza massiva billingovoy informatsii // Sbornik materialov XVI Vserossiyskoy nauchno-prakticheskoy konferentsii studentov, aspirantov i molodykh uchenykh «Bezopasnost' informatsionnogo prostranstva». – Yekaterinburg: UrFU, 2017 (v pechati).

5. Semenishchev I.A., Sinadskiy N.I. Statisticheskiye kharakteristiki sinteziruyemykh massivov billingovoy informatsii // Sbornik materialov XVI Vserossiyskoy nauchno-prakticheskoy konferentsii studentov, aspirantov i molodykh uchenykh «Bezopasnost' informatsionnogo prostranstva». – Yekaterinburg: UrFU, 2017 (v pechati).

6. Rao Zonghaoa, Yang Dongyuana, Duan Zhengyua. Resident Mobility Analysis Based on Mobile-Phone Billing Data // Procedia – Social and Behavioral Sciences, 96 (2013), S. 2032-2041.

СЕМЕНИЩЕВ Игорь Алексеевич, студент ИРИТ-РтФ УрФУ им. первого Президента России Б. Н. Ельцина; 620002, г. Екатеринбург, ул. Мира, 19. E-mail: semenishchevigor@mail.ru.

Синадский Алексей Николаевич, студент ИРИТ-РтФ УрФУ им. первого Президента России Б. Н. Ельцина; 620002, г. Екатеринбург, ул. Мира, 19. E-mail: alexsin@e1.ru.

Синадский Николай Игоревич, кандидат технических наук, доцент, доцент учебно-научного центра «Информационная безопасность» ИРИТ-РтФ УрФУ им. первого Президента России Б. Н. Ельцина; 620002, г. Екатеринбург, ул. Мира, 19. E-mail: nickis@e1.ru.

Сушков Павел Владимирович, аспирант ИЕНМ УрФУ им. первого Президента России Б.Н. Ельцина; 620002, г. Екатеринбург, ул. Мира, 19. E-mail: cyxapukob@gmail.com.

Semenishchev Igor, student of Institute of Radio electronics and Information Technologie,, Ural Federal University named after first President of Russia B.N. Yeltsin; 620002, Yekaterinburg, Mira str., 19. E-mail: semenishchevigor@mail.ru.

Sinadsky Alexey, student of Institute of Radio electronics and Information Technologies, Ural Federal University named after first President of Russia B.N. Yeltsin; 620002, Yekaterinburg, Mira str., 19. E-mail:alexsin@e1.ru.

Sinadsky Nikolay, candidate of technical sciences, associate Professor, Educational and Scientific Center "Information Security", Institute of Radio electronics and Information Technologies, Ural Federal University named after first President of Russia B.N. Yeltsin; 620002, Yekaterinburg, Mira str., 19. E-mail: nickis@e1.ru.

Sushkov Pavel, post-graduate student of Institute of Natural Sciences and Mathematics, Ural Federal University named after first President of Russia B.N. Yeltsin; 620002, Yekaterinburg, Mira str., 19. E-mail: cyxapukob@gmail.com.

УДК 004.056.2 + 342.7:004.056 + 005.7:004 Вестник УрФО № 1(27) / 2018, с. 57–62

Бердюгин В. Ю., Рясов Е. В.

ИСПОЛЬЗОВАНИЕ ВОЗМОЖНОСТЕЙ ИСУБД «CRONOSPRO» ДЛЯ ОРГАНИЗАЦИИ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ ПО ЗАЩИТЕ ИСПДН

В настоящей статье рассматриваются вопросы, связанные с организацией информационно-аналитического обеспечения деятельности по защите автоматизированной информационной системы, обрабатывающей конфиденциальную информацию. В качестве объекта исследования выбрана деятельность по обеспечению защиты информационной системы персональных данных (ИСПДн). Для удовлетворения информационных потребностей, возникающих при защите ИСПДн, предлагается использовать инструментальную систему управления базами данных «CronosPro». Для иллюстрации возможностей приводится пример учета машинных носителей персональных данных.

Ключевые слова: *информационная безопасность, персональные данные, инструментальная система, организационно–управленческая деятельность, информационно-аналитическое обеспечение, ИСУБД «CronosPro».*

USAGE OF IDBMS «CRONOSPRO» POSSIBILITIES FOR THE ORGANIZATION OF THE INFORMATION AND ANALYTICAL ASSURANCE ACTIVITY FOR IDBMS PROTECTION

In the given article there are the considered questions connected with the organization of the information and analytical assurance of the information security activity of the automated informational system working with confidential information. As an object of study was chosen the activity for IPBS protection. To satisfy the information needs, arising with IPBS protection, it is offered to use the Instrumental database management system «CronosPro».

Keywords: *information security, personal data, instrumental system, organizational management activity, information and analytical assurance, IDBMS «CronosPro».*

Деятельность по обеспечению информационной безопасности, как и другая организационно-управленческая деятельность, нуждается в информационном обеспечении. Формы и методы организационно-управленческой деятельности применяются в определенной последовательности, цикличности, диктуемой интересами и целями подготовки, принятием и исполнением управленческих решений. Этапы управленческой деятельности имеют логическую связь и образуют в совокупности следующий цикл управленческих действий:

• анализ и оценка управленческой ситуации;

• разработка и принятие управленческого решения;

• планирование исполнения принятых решений (разбиение на этапы, назначение ответственных);

• организация и контроль выполнения принятых решений;

• обобщение результатов проведенной управленческой деятельности, оценка новой (результирующей) управленческой ситуации [1].

Организационно–управленческую деятельность по обеспечению безопасности информационной системы персональных данных (ИСПДн), в соответствии с Федеральным законом «О персональных данных» [2], условно можно разделить на два цикла:

1. До начала эксплуатации информационной системы:

• определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

• применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивают установленные Правительством Российской Федерации уровни защищенности персональных данных;

• применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

• оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.

2. После ввода в эксплуатацию информационной системы:

• обучение персонала по работе с информационной системой персональных данных;

• учет машинных носителей персональных данных;

• установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных.

• обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;

• восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

• контроль над принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;

Перечисленные виды деятельности нуждаются в информационно-аналитическом обеспечении.

Под информационно-аналитическим обеспечением деятельности по защите ИСПДн понимается комплекс мероприятий и приёмов по изучению и оценке определённой совокупности информации, характеризующей состояние информационной системы, результаты деятельности подразделений информационной безопасности по выполнению стоящих перед ними задач, а также условий, в которых данные задачи решаются.

Исходя из перечня мер, обеспечивающих защиту ИСПДн, указанных в постановлении Правительства Российской Федерации от 01.11.2012 № 1119 [3] и приказе Федеральной службы по техническому и экспортному контролю России от 18.03.2013 № 21 [4], специалисту по защите информации необходимо обеспечить:

Относительно функции информационной системы по загрузке, хранению и извлечению данных:

• ведение базы данных, содержащих информацию обо всех лицах, взаимодействующих с ИСПДн;

• ведение и поддержку актуального состояния документационного обеспечения системы безопасности ИСПДн;

• учет носителей персональных данных (ПД);

• накопление информации о проведении инструктажа сотрудников;

• учет результатов служебных разбирательств, по фактам нарушения требований информационной безопасности.

Относительно функции информационной системы по решению информационно-логических задач:

• учёт осведомленности сотрудников организации;

• выявление инцидентов, связанных с нарушениями требований безопасности ИСПДн.

• контроль наличия носителей ПД у сотрудников организации;

• фиксацию взаимодействий организации со сторонними учреждениями (юридическими лицами, органами, осуществляющими контроль защищенности ИСПДн);

• выявление скрытых связей при проведении компьютерной экспертизы.

Определяющей тенденцией в сфере обеспечения информационной безопасности является создание баз данных для выполнения требований законодательства Российской Федерации [5].

В частности, когда речь идет об обеспечении информационно-аналитической деятельности по защите ИСПДн большую роль играет выбор системы управления базами данных (СУБД) как непосредственной системы обработки защищаемой информации. Необходимо отметить, что к данному инструменту также предъявляются требования соответствия положениям нормативной правовой базы в сфере информационной безопасности.

Нами проведён сравнительный анализ СУБД, располагающих набором соответствующих возможностей, которые представлены в виде таблицы (см. табл. 1).

В результате нами выбрана инструментальная система управления базами данных ИСУБД «CronosPRO» как наиболее подходящее средство решения поставленной задачи, так как ключевыми особенностями системы являются:

• наличие инструментов проектирования структуры банков данных;

• возможность ввода/коррекции данных с использованием настраиваемых пользователем форм или стандартных средств;

• визуализация построения сложных запросов с использованием различных критериев и условий, в том числе по нескольким связанным базам данных;

• поддержка одновременного поиска по множеству информационных массивов;

• возможность создания, хранения и использования шаблонов запросов;

Таблица 1

Сравнительные характеристики СУБД

СУБД / Функции	Линтер	CronosPRO	Oracle MySQL
Оперативное удовлетворение информационных потребителей	+	+	+
Непрерывность процесса отбора и переработки информации	-	+	+
Отсутствие дублирования информации	+	+	+
Контроль корректности информации	-	+	+
Приведение обрабатываемых сведений к общему формату	-	+	+
Фильтрация, агрегирование и актуализация информации	-	+	+
Цена	От 25 000 руб	8500 руб (на 10 лет)	≈ 130 000 руб (на 1 год)
Наличие сертификатов	Министерство обороны РФ, ФСТЭК	ФСБ, ФСТЭК	Отсутствуют

• наличие средств визуального отображения и анализа взаимосвязей между объектами;

• поддержка работы с данными внешних форматов (MS Access, MS Excel, Oracle, XML и др.);

• наличие гибкой системы обеспечения безопасности хранимой информации, выполняющей задачи аутентификации пользователей, разграничения доступа к объектам ИСУБД и регистрации происходящих событий;

• возможность автоматического выполнения ряда операций (ревизии, резервного копирования, оптимизации, индексации и др.) по расписанию или в режиме контроля файлов [6].

Для решения информационно-аналитических задач сотрудникам подразделения защиты информации нами создан банк данных, который содержит в себе следующие взаимосвязанные базы данных:

• лиц;

• организаций;

• действий;

• носителей.

Разработаны входные формы для ввода информации, библиотека запросов для решения типовых информационно-логических задач и инструкции пользования банком данных.

В качестве примера рассмотрим организацию информационно-аналитического процесса по учету машинных носителей ПД.

В тексте, при построении алгоритма, используются следующие сокращения, обозначения, символы:

О – ответственный;

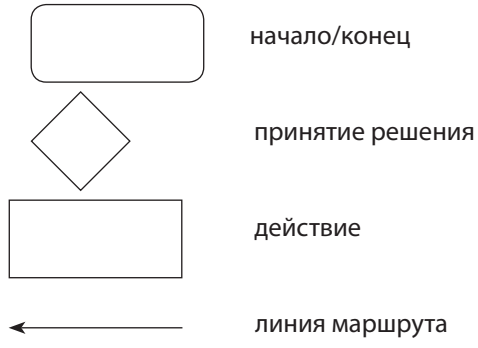
И – исполнитель;

У – участник;

Рук – руководитель организации;

Сотр – сотрудник организации;

Спец – специалист по защите информации в организации.



1. Рук, на основании предложения от Сотр, принимает решение о регистрации носителя.

2. Носитель регистрируется Спец, который вносит информацию в БД.

3. Спец выдает Сотр носитель, факт выдачи фиксируется в БД.

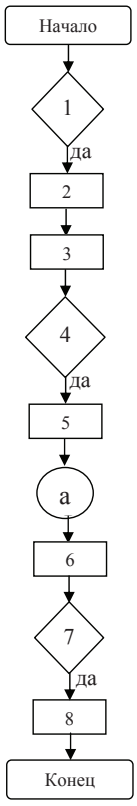
4. При возникновении необходимости передачи носителя от Сотр 1 к Сотр 2, Рук, на основании предложения Сотр 1, принимает решение о передаче.

5. После получения разрешения Сотр 1 сдает носитель Спец, который выдает носитель Сотр 2, о чем делается запись в БД.

6. При необходимости уничтожения носителя Сотр выходит с соответствующим предложением к Рук, который принимает решение об уничтожении носителя.

Таблица 2

Алгоритм действий



Действия	О	И	У
1. Принятие решения о регистрации носителя (1)	Рук.	Спец.	Сотр.
2. Регистрация носителя (2)	Спец.	Спец.	Сотр.
3. Выдача носителя (3)	Спец.	Спец.	Сотр.
4. Принятие решения о передаче (4)	Рук.	Сотр. 1	–
5. Прием носителя (5)	Спец.	Сотр. 1	–
6. Выдача носителя (5)	Спец.	Сотр. 2	–
7. Принятие решения об уничтожении носителя (6)	Рук.	Сотр.	Сотр.
8. Уничтожение носителя (7,8)	Рук.	Спец.	Сотр .1 Сотр. 2

7. Сотр сдает носитель Спец, после чего создается комиссия, составляется акт уничтожения, утверждаемый Рук.

8. Комиссия производит уничтожение носителя, в БД Спец заносит информацию о выведении носителя из работы.

БД лиц формируется из руководителя, специалиста и сотрудников организации. БД действий формируется из регистрации, выдачи, приема и уничтожения носителя. БД носителей формируется из электронных носителей информации (CD, DVD, Blu-ray диски; флэш-память, SSD-диски, дискеты, жесткие диски). Все процессы, связанные между собой, происходят в одной организации. Лица будут являться участниками действий, которые происходят с носителем, который в каждый момент времени закреплён за конкретным лицом.

Таким образом, в информационно-аналитической системе будет накапливаться структурируемая информация, которая поможет решать следующие информационно-справочные и информационно-логические задачи:

- накапливать информацию о количестве носителей конфиденциальной информации;
- определять наличие их у сотрудников организации;
- устанавливать количество выведенных из работы носителей.

В результате в любой момент можно получить информацию о том, какое количество сотрудников работало с определённым носителем, и наоборот, с какими носителями работал каждый сотрудник.

Подобным образом, будет функционировать система по отношению к остальным мерам защиты ИСПДн. Построение БД с использованием одних и тех же взаимосвязанных информационных объектов поможет специалисту по защите информации решать сложные информационно-аналитические задачи в том числе выявлять скрытые связи между объектами.

Литература

1. Организация государственного управления – стадии управленческой деятельности. Экономическая энциклопедия. Российская библиотека. – URL: http://economedu.ru/gosupravlenie/159-oraganizacia-upravlenia.html?start=17 (дата обращения: 04.09.2017);

2. О персональных данных: Федеральный закон № 152-ФЗ от 27.07.2006 (с изм. и доп.). – URL: http://www.consultant.ru/document/cons_doc_LAW_61801 (дата обращения: 09.11.2017);

3. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства № 1119 от 01.11.2012 (с изм. и доп.). – URL: http://www.consultant.ru/document/cons_doc_LAW_137356 (дата обращения: 09.11.2017);

4. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ ФСТЭК России № 21 от 18.03.2013 (с изм. и доп.). – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 09.11.2017);

5. Мищенко Е. Ю., Соколов А. Н. Количественный анализ процедуры обезличивания персональных данных. Метод перемешивания // Вестник УрФО «Безопасность в информационной сфере». 2016. № 3 (21). 30 с.

6. ИСУБД «CronosPRO» URL: http://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:CronosPRO (дата обращения: 11.09.2017).

References

1. Organizatsiya gosudarstvennogo upravleniya – stadii upravlencheskoy deyatel'nosti. Ekonomicheskaya entsiklopediya. Rossiyskaya biblioteka. URL: http://economedu.ru/gosupravlenie/159-oraganizacia-upravlenia.html?start=17 (data obrashcheniya: 04.09.2017).

2. O personal'nykh dannykh: Federal'nyy zakon № 152-FZ ot 27.07.2006 (s izm. i dop.). URL: http://www.consultant.ru/document/cons_doc_LAW_61801 (data obrashcheniya: 09.11.2017).

3. Ob utverzhdenii trebovaniy k zashchite personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh: Postanovleniye Pravitel'stva № 1119 ot 01.11.2012 (s izm. i dop.). URL: http://www.consultant.ru/document/cons_doc_LAW_137356 (data obrashcheniya: 09.11.2017).

4. Ob utverzhdenii sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh: Prikaz FSTEK Rossii № 21 ot 18.03.2013 (s izm. i dop.). URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (data obrashcheniya: 09.11.2017).

5. Mishchenko Ye.YU., Sokolov A.N. Kolichestvennyy analiz protsedury obezlichivaniya personal'nykh dannykh. Metod peremeshivaniya // Chelyabinsk: Vestnik UrFO «Bezopasnost' v informatsionnoy sfere» № 3(21), 2016. 30 s.

6. ISUBD «CronosPRO» URL: http://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:CronosPRO (data obrashcheniya: 11.09.2017).

БЕРДЮГИН Владимир Юрьевич, доцент кафедры защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, пр. Ленина, д. 76. E-mail: bvu55@mail.ru.

РЯСОВ Евгений Владимирович, студент кафедры защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, пр. Ленина, д. 76. E-mail: Ryasov_zheny@mail.ru.

BERDYUGIN Vladimir, docent of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76,Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: bvu55@mail.ru.

RYASOV Evgeniy, student of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: Ryasov_zheny@mail.ru.

УДК 004:338 + 004.738.5:336.743 + 004.056.5 Вестник УрФО № 1(27) / 2018, с. 63–65

Емцева С. С., Морозов Н. В.

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ICO В РОССИЙСКОЙ ФЕДЕРАЦИИ

В статье дан обзор новому инструменту привлечения капитала — понятию ICO (Initial Coin Offering). Рассмотрены тенденции правового регулирования ICO в Российской Федерации.

Ключевые слова: *криптовалюта, биткоин, блокчейн, ICO, безопасность, платежи, финансовые технологии.*

Emtseva S. S., Morozov N. V.

LEGAL REGULATION OF ICO IN THE RUSSIAN FEDERATION

The article gives an overview of a new tool for raising capital – the concept of ICO (Initial Coin Offering). The tendencies of the legal regulation of the ICO in the Russian Federation are considered.

Keywords: *crypto currency, bitcoin, blockchain, ICO, security, payments, financial technologies.*

Каждый из нас имеет возможность осуществлять платежи через Сеть. Но в этих процессах участвуют неэффективные, устаревшие системы, которые очень медлительны, а все операции выполняются централизованно. У компьютеров в виду их постоянного взаимодействия должна быть возможность быстрого производства миллиардов микроплатежей друг другу, расплачиваясь электроэнергией и местом в хранилище, а не огромными гонорарами за услуги посредников. Именно эту проблему помогает решить биткоин (Bitcoin) — полезный инструмент для оперативного перечисления средств [1]. В 2017 году минуло 9 лет, как аноним, использовавший вымышленное имя Сатоси Накамото (Satoshi Nakamoto), разработал протокол биткоина и первую версию программного обеспечения, в котором этот протокол был организован. Развитие криптовалют, начавшееся с того времени, неизменно влекло появление новых технологий, способов инвестиций и заработков, и одним из таких способов стало ICO (Initial Coin Offering).

ICO без преувеличения можно назвать финансовой темой 2017-ого года. Получение финансирования через него приобрело значительные масштабы — только за первое полугодие было привлечено более $1 млрд [2]. Популяризация ICO (рис. 1) вызвана, во-первых, тем, что рынок криптовалют гораздо демократичнее традиционного рынка ценных бумаг, а, во-вторых, тем, что интерес со стороны государства к технологии блокчейн (Blockchain), базе данных с широкомасштабным тиражированием всех транзакций в сети биткоин [1], постоянно растет.

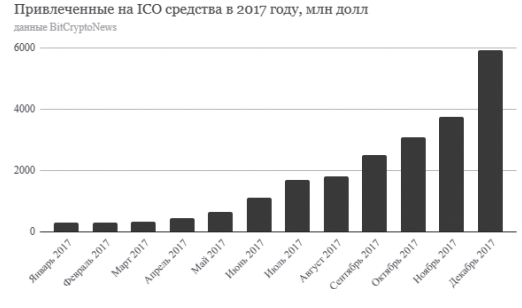


Рис. 1. «Привлеченные на ICO средства в 2017 гг., млн долл»[1]

[1] Данные BitCryptoNews.

ICO (Initial Coin Offering) — дословно «первичный выпуск монет» [2] — это инструмент привлечения капитала за счет вовлечения инвесторов в стартап, который занимается разработкой и продвижением какого-либо сервиса/технологии/платформы, связанного с криптовалютой. О начале проведения ICO обычно объявляется на профильных криптовалютных форумах (bitcointalk.org), на которые выкладывают всю ключевую и техническую информацию о проекте: цель, временные рамки проведения ICO, команда, особенности проекта, дорожная карта развития площадки и прочие детали. Выпуск происходит путем добавления в блокчейн транзакции с их описанием, количеством и уникальным ID. Привлечение капитала происходит за счет предварительной распродажи по установленной организатором ICO цене так называемых токенов — цифровых жетонов. При этом ценность токенов не гарантирует никто, кроме компании, их выпустившей. Инвесторы — пользователи платформы — покупают токены, платя за них криптовалютой. В будущем для инвесторов есть несколько путей развития событий касаемо токенов: либо расплачиваться ими на более выгодных условиях за услуги внутри платформы, либо, дождавшись, когда эти токены вырастут в цене, выйти с ними на биржу и обменять на другие криптовалюты или фиатные деньги, и, таким образом, получить прибыль.

На данный момент правовой статус ICO не определен ни в одной стране — инвесторы никак юридически не защищены в случае провала на рынке объекта своего финансирования. Анонимность транзакций и отсутствие регуляторов в лице государственных органов — темная сторона рынка блокчейна и криптовалют, позволяющие использовать криптобиржи для отмывания денег и финансирования криминальных структур. Сегодня правительства только пробуют с этим бороться, и эффективность их действий оценить трудно.

В России правовой статус криптовалют не определен. Статья 75 Конституции РФ запрещает денежные суррогаты, к которым при желании регуляторов можно отнести биткоин и его аналоги. Тем не менее, технология блокчейн, лежащая в основе криптовалют, не запрещена. Хотя Роскомнадзор неоднократно выступал с предложениями запретить использование биткоина в России, на данный момент Банк России обсуждает вопрос о признании биткоина с Министерством финансов и Росфинмониторингом.

Осенью президент Российской Федерации Владимир Владимирович Путин дал поручение правительству и Центральному Банку подготовить поправки в законодательство, которые бы регламентировали порядок налогообложения и регистрации компаний, занимающихся майнингом, а так же порядок регулирования ICO по аналогии с регулированием публичной продажи акций акционерного общества [4]. Стал вопрос в необходимости определения статуса цифровых технологий таких как «криптовалюта», «токен», «цифровая закладная» и другие. Соответствующие поправки должны быть внесены в законодательство до 1 июля 2018 года. А до конца декабря 2017 года на базе ЦБ должна быть создана специальная регулятивная площадка для апробации инновационных финансовых технологий.

Тем временем Государственная Дума объявила открытый конкурс на проведение экспертно-аналитического исследования по теме «Законодательное регулирование внедрения и практического применения современных финансовых технологий». Победителем в конкурсе стал Финансовый университет при Правительстве РФ. Предполагается, что его исследования будут использованы Госдумой для формирования законодательных инициатив по интеграции и законодательному обеспечению наиболее перспективных финансовых технологий, их развитию и регулированию.

Снизить риски ICO-инвесторов помогло бы не только законодательное регулирование, но и создание специальных рейтинговых агентств. Организованная в начале осени российская ассоциация криптовалют и блокчейна (РАКИБ) основным полем деятельности выбрала формирование «законодательного поля для участников новой блокчейн-индустрии», и одной из первых выдвинула идею создания рейтингового агентства для компаний и проектов, которые проводят ICO [5]. В будущем планируется синхронизация законов с законодательствами других стран для разработки единых стандартов регулирования ICO.

Говоря об ICO как об инструменте привлечения капитала, а так же средстве получения прибыли, необходимо осветить вопрос налогообложения, особый порядок которого главой 23 «Налог на доходы физических лиц»

Кодекса не установлен. Тем не менее, Министерство финансов Российской Федерации дает ссылку статью 228 Налогового кодекса, в которой говорится о самостоятельном исчислении суммы налога, подлежащего уплате в соответствующий бюджет.

Таким образом, наблюдается тенденция стремления правительства Российской Федерации легализовать сектор ICO, чтобы обеспечить инновационную деятельность, разнообразное развитие бизнеса и доход от ICO. По мере того, как правительство стремится создать выгодные условия для ICO, оно изучает ряд правовых и нормативных шагов, которые уже приводят к соответствующему балансу защиты рынка и инвесторов в сочетании со структурами, необходимыми для продолжения развития отрасли. Государственный регулятор пытается нащупать наиболее эффективную модель регулирования операций с криптовалютами. Чего ждать от российского законодательства должен показать 2018 год. Очевидно, что чем быстрее и успешнее Российская Федерация реализует регуляцию ICO, тем больше инвесторов она привлечет и тем большую доходность получит.

Литература

1. Равел, С. Децентрализованные приложения. Технология Blockchain в действии / С. Равел. – СПб. : Питер, 2017. – 240 с.

2. «DeCenter ICO Book 2017» / Е. Гордеев, А. Поддубняк, А. Прохоров и др. – 2017. – 34 с.

3. Оганесов, А. «Путин поручил разработать налоги на майнинг криптовалют» / А. Оганесов // РБК, 1995–2017. – URL: http://www.rbc.ru/rbcfreenews/59ef17b19a7947cbc27e0b6d (Дата обращения: 09.11.2017 г.)

4. Балашова, А. «В России начали создавать первые рейтинговые агентства под ICO» / А. Балашова, А. Криворотова, Г. Казакулова // РБК, 1995–2017. – URL:http://www.rbc.ru/technology_and_media/14/09/2017/59b9574d9a794758483e3b44 (Дата обращения: 10.11.2017 г.)

References

1. Ravel S. Decentralized applications. Technology Blockchain in action / S. Ravel – St. Petersburg. : Peter, 2017. – 240 p.

2. DeCenter ICO Book 2017 / E. Gordeev, A. Poddubnyak, A. Prokhorov, E. Yakubov, P. Mishin, Sergey Alexandrovich. – 2017. – 34 p.

3. Oganesov A. "Putin instructed to develop taxes on the mining of crypt-lute" // RBC, 1995-2017. Available at: http://www.rbc.ru/rbcfreenews/59ef17b19a7947cbc27e0b6d

4. A. Balashova, A. Krivorotova, G. Kazakulova "In Russia, the first rating agencies were created under the ICO" // RBC, 1995–2017. Available at: http://www.rbc.ru/technology_and_media/14/09/2017/59b9574d9a794758483e3b44

ЕМЦЕВА Софья Сергеевна, студентка 2-го курса, Институт интеллектуальных и кибернетических систем, Национальный исследовательский ядерный университет «МИФИ», 115409, г. Москва, Каширское шоссе, д. 31. E-mail: sofochkaemtseva@mail.ru

МОРОЗОВ Николай Владимирович, кандидат юридических наук, доцент кафедры Финансового мониторинга, Национальный исследовательский ядерный университет «МИФИ», 115409, г. Москва, Каширское шоссе, д. 31.

EMTSEVA Sofya, 2-year student, Institute of Cyber Intelligence Systems, National Research Nuclear University MEPhI. Bld. 31, Kashirskoe Rd., Moscow, 115409. E-mail: sofochkaemtseva@mail.ru

MOROZOV Nikolay, Candidate of Juridical Sciences, Associate Professor at the Department of Financial Monitoring, National Research Nuclear University MEPhI. Bld. 31, Kashirskoe Rd., Moscow, 115409.

УДК 004.056.53 + 004.4.056 Вестник УрФО № 1(27) / 2018, с. 65–70

Муравьев Н. С., Астахова Л. В.

ПРОФИЛАКТИКА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ПРОФИЛИРОВАНИЯ ПОЛЬЗОВАТЕЛЕЙ: ПРОГРАММНО-ТЕХНИЧЕСКИЙ АСПЕКТ

В статье рассмотрена проблема профилирования пользователей информационной системы как средства профилактики инцидентов в сфере информационной безопасности (ИБ). Предложены направления для технической реализации профилирования. Обоснованы критерии оценки поведения пользователей информационной системы (ИС), имеющие количественную характеристику. Определена возможность автоматизации профилирования и прогнозирования возможных инцидентов ИБ по вине каждого отдельно взятого пользователя ИС. Предложен алгоритм прогнозирования тенденции в поведении пользователя. В качестве инструмента определения степени уязвимости пользователя обоснован «Профайл безопасного пользователя».

Ключевые слова*: информационная безопасность, поведение пользователя, профайлинг, профилирование, профайл, инциденты, пользователь, машинное обучение, прогнозирование поведения.*

Muravyov N. S., Astakhova L. V.

PREVENTION OF INFORMATION SECURITY INCIDENTS BASED ON USER PROFILING: PROGRAM-TECHNICAL ASPECT

The article considers the problem of profiling users of the information system as a means of preventing incidents in the field of information security. Suggested directions for technical implementation of profiling. The criteria for assessing the behavior of IP users, which have a quantitative characteristic, are substantiated. The possibility of automation of profiling and forecasting of possible IS incidents through the fault of each individual IP user has been determined. An algorithm for predicting the trend in user behavior is proposed. The «Safe User Profile» is justified as a tool for determining the vulnerability of a user.

Keywords: *information security, user behavior, profiling, profiling, profile, incidents, user, machine learning, behavior prediction.*

The work was supported by Act 211 Government of the Russian Federation, contract № 02. A03.21.0011

Человеку отводится ключевая роль в процессах организации, функционирования и развития деятельности коммерческих и государственных организаций, предприятий и иных структур. В процессе деятельности сотрудник располагает совокупностью информационных ресурсов организации, а также имеет доступ к средствам ее обработки, которые могут вызвать интерес не только у правообладателя, но и третьих лиц. В целях сохранности ключевой информации в организациях вводится режим информационной безопасности (далее – ИБ), который состоит из правовых, организационных и программно-технических мер защиты.

Большая часть выявленных нарушений информационной безопасности происходит из-за человеческого фактора в информационной системе (далее – ИС). Это подтверждают статистические исследования компании InfoWatch. Например, за 2016 год по причине внутреннего нарушителя было реализовано около 62 % угроз [5]. Под человеческим фактором мы понимаем набор преднамеренных или неумышленных (например, при неправильной эксплуатации ИС) действий внутреннего пользователя, в результате которых реализуется угроза и происходит утечка информации.

В повседневной рабочей среде при длительном периоде без инцидентов в ИБ, а также при отсутствии видимых угроз у пользователя меняется восприятие опасностей. Это приводит к успешной реализации социальной инженерии, фишинга, инсайдерских утечек и т. д., которые предполагают наличие человеческого воздействия на систему. Подобные угрозы усложняются тем, что внутренний пользователь имеет прямой доступ к информации и его поведение с меньшей вероятностью отличается от нормы. Поэтому в последние годы повысился интерес к оценке кадровых уязвимостей информационных систем [1], в том числе на основе профайлинга [6].

Анализ российской и зарубежной литературы показал, что зачастую профайлинг рассматривается с позиций гуманитарно-психологического подхода: в деятельности кадровых служб [2], в правоохранительной деятельности [3] и др. Профайлингу в сфере ИБ уделяется значительно меньше внимания. Этим обусловлена цель данной работы – обосновать программно-техническое решение профилирования пользователей как средство профилактики инцидентов информационной безопасности. В числе задач статьи – определение критериев для оценки поведения пользователя при взаимодействии с ИС для последующего прогнозирования тенденции его поведения; обоснование алгоритма прогнозирования тенденции ИБ-поведения пользователя на основе предложенного «Профайла безопасного пользователя».

Зарубежные специалисты рассматривают профайлинг и профилирование с позиции, основанной на криминалистических подходах [4]. На наш взгляд, профилирование – процесс сбора и накопления данных о пользователях, структурированных по атрибутам согласно определенным критериям оценки с целью прогнозирования поведения пользователей. Профайл – это результат профилирования: совокупность записей в базе данных с атрибутами, содержащими критерии для оценки поведения по каждому пользователю ИС.

Достижение обозначенной цели возможно путем смешения социальных и технологических решений, результаты которых должны вноситься в профайл каждого отдельного взятого сотрудника организации.

К социальным решениям относятся такие данные, как сведения о психологических, социальных, культурных и иных гранях жизни человека. Данные об этом собираются через опросы, тесты, наблюдения и иные формы внутренних и внешних проверок. К технологическому решению относится раздел, который исследует непосредственно поведение человека в момент, когда он является пользователем ИС [4].

Мы рассмотрим идею программно-технического профилирования пользователя как дополнение к различным системам мониторинга или DLP-системам. В совокупности эти данные вносятся в профайл для определения поведенческого типа каждого сотрудника. При анализе данных из профайла изучается поведение сотрудника, соответствие степени соблюдения политики информационной без-

опасности организации, уровень лояльности и прочие поведенческие качества для дальнейшего прогнозирования.

Для разработки программно-технических средств профилирования необходимо четкое определение критериев. Зарубежные специалисты выделяют такие критерии оценки поведения пользователя, как:

1) обращение с паролями (оценка изменения пароля и его надежность в соответствии с установленной политикой безопасности);

2) периодичность резервного копирования (своевременность резервного копирования в случае наличия таких обязанностей на пользователе [4].

Мы считаем, что перечень этих критериев может быть расширен на основе используемых сведений о пользователях, собираемых в DLP-системах и других системах с возможностью мониторинга, применяемых в российской и зарубежной практике защиты информации. К таким критериям мы относим:

- данные о попытках доступа к сектору информации ограниченного доступа для пользователя;
- данные о сетевой активности и сопоставление просматриваемых интернет-ресурсов на предмет отношения к профессиональной деятельности;
- сведения о попытках взаимодействия со съемными носителями;
- регистрация запросов к установленным средствам защиты информации (например, данные о попытке просмотра настроек средства от НСД, антивируса и т. д.);
- количество инцидентов, аномалий и т. д., зафиксированных DLP-системой;
- иные сведения, которые могут быть получены в процессе мониторинга.

Указанный перечень критериев может быть расширен в соответствии с технологическими возможностями каждой отдельной организации.

На основе указанных критериев предлагаем сформировать так называемый «Профайл безопасного пользователя». В нем должны содержаться оптимальные показатели указанных критериев, которые соответствуют установленным требованиям Политики ИБ. Например, такими показателями могут быть установленная периодичность смены паролей пользователей, количество попыток несанкционированного доступа к защищаемой информации и др.

Представим общую схему профилирования, оценки и прогнозирования поведения пользователя ИС (рис. 1).

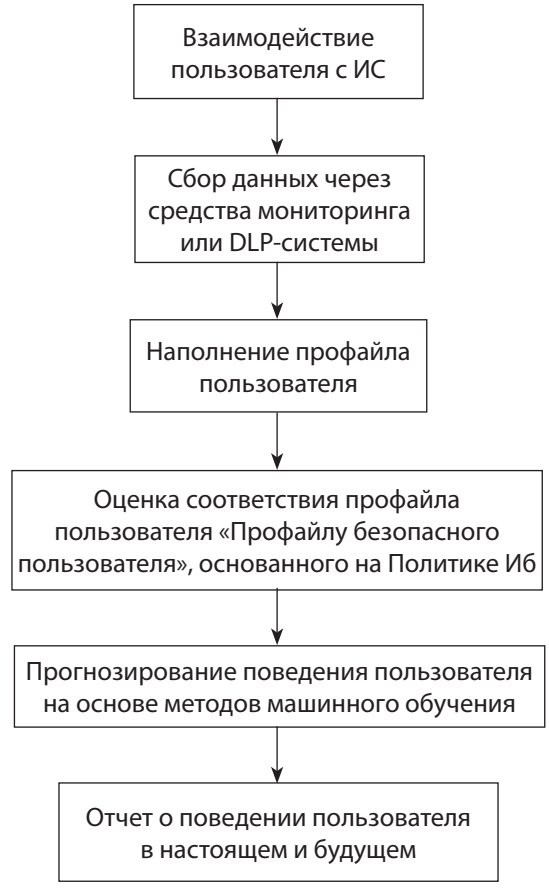


Рис. 1 Общая схема профилирования, оценки и прогнозирования поведения пользователя ИС

Более подробно рассмотрим процесс прогнозирования. Для этого предлагаем применить методы машинного обучения и считать полученную программу частью «Профиля безопасного пользователя», а полученные показатели – учитывать при дальнейшей оценке пользователя.

Машинное обучение – моделирование признаков данных и соответствующих данным меток. Данное определение относится к категории задач «обучение с учителем», когда некоторые прогнозируемые данные частично известны [7].

Сформулируем задачу: на основе данных за два месяца работы пользователя спрогнозировать уровень его угрозы ИБ на предстоящий месяц с помощью компонента для прогнозирования «Профиля безопасного пользователя».

Для решения задачи применяются библиотеки:

• Pandas,
• Numpy,
• Scikit-Learn на языкеPython.

Уровень угрозы рассчитывается как:

$$\text{Уровень угрозы(за месяц)} =$$

$$= \frac{\text{Количество угроз за месяц}}{\text{Кличество дней в месяце}} * 100$$

Собранные данные поступают в программу для прогнозирования в следующем виде (рис. 2):

Дата	Инциденты	Аномалии	Опоздания	Отсутствие	Статус
01.09.2017	0	0	0	0	0
02.09.2017	1	0	0	0	1
03.09.2017	0	0	0	1	0
04.09.2017	0	0	0	0	0
05.09.2017	0	0	0	0	0
06.09.2017	1	1	0	1	1
07.09.2017	0	0	0	0	0
08.09.2017	0	0	0	0	0
09.09.2017	2	0	1	0	1

Рис. 2. Пример части данных для прогнозирования

Представленные данные необходимо разделить на матрицу признаков (X) и целевой вектор (Y).

Матрица признаков – набор столбцов: инциденты, аномалии, опоздания, отсутствие на рабочем месте (заранее выбранные критерии для прогнозирования).

Целевым вектором является столбец «Статус», значения которого и будут спрогнозированы, где 0 – пользователь не являлся угрозой, 1 – пользователь являлся угрозой. В данном случае пользователя считали угрозой ИБ, если у него был, хотя бы один инцидент.

На основе уже заполненного целевого вектора за сентябрь и октябрь рассчитаем для них уровень угрозы пользователя:

• Сентябрь

```
In [165]: print (september_result,"% уровень угрозы за сентябрь")
18 % уровень угрозы за сентябрь
```

• Октябрь

```
In [168]: print (october_result,"% уровень угрозы за октябрь")
13 % уровень угрозы за октябрь
```

Алгоритм прогнозирования представим в виде следующих этапов (далее указаны только основные функции программы):

1. Выбор модели: «Гауссов наивный байесовский классификатор»:
from sklearn.naive_bayes import GaussianNB;

Выбранная модель «Гауссов наивный байесовский классификатор» – модель из категории «обучение с учителем», т. е. целевой массив изначально уже имеет значения, на основе которых прогнозируются значения на будущий месяц. Данные классифицируются относительно целевого вектора «Статус».

2. Создание экземпляра модели:
model = GaussianNB()
3. Обучение модели:
model.fit(X_dlp, Y_dlp)
4. Предсказание значений:
november = model.predict(X_dlp)
5. Расчет и вывод результата:
november_result =
round((sum/november.size)*100)

```
In [62]: print ("Прогнозируем", november_result,"% уровень угрозы за ноябрь")
Прогнозируем 23 % уровень угрозы за ноябрь
```

Мы видим, что прогноз уровня угрозы ИБ со стороны данного пользователя на месяц ноябрь составляет 23 %. А это значит, что прогнозируется повышение тенденции на 10 % относительно октября. Это можно расценивать как повышение угрозы со стороны данного пользователя.

Таким образом, важным средством профилактики инцидентов ИБ является профилирование пользователей. Обоснованные критерии оценки поведения пользователей ИС имеют количественную характеристику. Это обеспечивает возможность автоматизации профилирования и прогнозирования возможных инцидентов ИБ по вине каждого отдельно взятого пользователя ИС. В статье обоснован алгоритм прогнозирования тенденции в ИБ – поведении пользователя, под которой понимается разница в показателе оценки уровня угрозы пользователя на выбранный прогнозируемый период. В качестве инструмента определения степени уязвимости пользователя предложен «Профайл безопасного пользователя».

Литература

1. Астахова Л. В. и др. Автоматизация многофакторной оценки кадровых уязвимостей информационной безопасности / Л. В. Астахова, В. А. Ефремов, А. И. Митькин // Вестник УрФО. Безопасность в информационной сфере. – 2014. - № 4 (14). – С. 57–61.

2. Арпентьева М. Р. Профайлинг как современная HR-технология // Инновационное развитие современных социально-экономических систем материалы III Международной заочной научно-практической конференции. – 2016. – С. 296–301.

3. Черкасова Е.С. Профайлинг как метод создания психологического портрета потенциального преступника на этапе организации предварительного расследования // Юридическая наука и практика. – 2013. – С. 72–75.

4. Fernando S. A. Securing Information Sharing Through User Security Behavioral Profiling / S. A. Fernando, Takashi Yukawa // Transactions on Engineering Technologies. – 2013. – С. 655–670.

5. Глобальное исследование утечек конфиденциальной информации в 2016 году. – URL: https://www.infowatch.ru/analytics/reports/17479 (дата обращения: 10.01.2018).

6. Бируля И. Как оцифровать человеческий фактор // Журнал «Information Security/ Информационная безопасность». – 2017. – № 4. – URL: http://www.itsec.ru/articles2/sys_ogr_dost/kak-otsifrovat-chelovecheskiy-faktor

7. Плас Дж. Вандер. Python для сложных задач: наука о данных и машинное обучение. — СПб. : Питер, 2018. – 576 с.

Referenses

1. Astahova L.V. i dr. Avtomatizaciya mnogofaktornoj ocenki kadrovyh uyazvimostej informacionnoj bezopasnosti / L. V. Astahova, V.A. Efremov, A.I. Mit'kin // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. – 2014. – № 4 (14). – S. 5–61.

2. Arpent'eva M. R. Profajling kak sovremennaya HR-tekhnologiya // Innovacionnoe razvitie sovremennyh social'no-ehkonomicheskih sistem materialy III Mezhdunarodnoj zaochnoj nauchno-prakticheskoj konferencii. -2016.- S. 296-301.

3. CHerkasova E.S. Profajling kak metod sozdaniya psihologicheskogo portreta potencial'nogo prestupnika na ehtape organizacii predvaritel'nogo rassledovaniya// YUridicheskaya nauka i praktika.-2013.-S.72-75.

4. Fernando S. A. Securing Information Sharing Through User Security Behavioral Profiling / S. A. Fernando, Takashi Yukawa // Transactions on Engineering Technologies. – 2013. – P. 655–670.

5. Global'noe issledovanie utechek konfidencial'noj informacii v 2016 godu – https://www.infowatch.ru/analytics/reports/17479 – (data obrashcheniya: 10.01.2018).

6. Birulya I. Kak ocifrovat' chelovecheskij faktor // ZHurnal "Information Security/ Informacionnaya bezopasnost'". – 2017. – № 4. http://www.itsec.ru/articles2/sys_ogr_dost/kak-otsifrovat-chelovecheskiy-faktor

7. Plas Dzh. Vander. Python dlya slozhnyh zadach: nauka o dannyh i mashinnoe obuchenie. — SPb.: Piter, 2018. — 576 s.

МУРАВЬЕВ Никита Сергеевич, студент кафедры защиты информации Южно-Уральского государственного университета. 454080, г. Челябинск, пр. Ленина, д. 76. E-mail: mns7496@yandex.ru

АСТАХОВА Людмила Викторовна, доктор педагогических наук, профессор, профессор кафедры защиты информации Южно-Уральского государственного университета. 454080, г. Челябинск, пр. Ленина, д. 76. E-mail: lvastachova@mail.ru

MURAVYOV Nikita, student of the Department of Information Security South Ural State University. 454080, Chelyabinsk, Lenin Avenue, 76. E-mail: mns7496@yandex.ru

ASTAKHOVA Lyudmila, doctor of pedagogical sciences, professor, professor of the department of information protection South Ural State University. 454080, Chelyabinsk, Lenin Avenue, 76. E-mail: lvastachova@mail.ru

УДК 004.056.57
ББК Х404.06 + 79(2)-983

Вестник УрФО № 1(27) / 2018, с. 71–76

Ванцева И. О., Зырянова Т. Ю., Медведева О. О.

ВЛИЯНИЕ ФЕДЕРАЛЬНОГО ЗАКОНА «О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ» НА ВЛАДЕЛЬЦЕВ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР

В статье рассмотрены актуальные вопросы, связанные с выходом федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», а также отражены основные аспекты категорирования объектов критической информационной инфраструктуры, о котором говорится в Постановлении Правительства от 08.02.2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений», также в статье указано, что такое ГосСОПКА, для чего создана и какие функции должна выполнять.

Ключевые слова: *критическая информационная инфраструктура, информационная безопасность, категорирование объектов.*

INFLUENCE OF THE FEDERAL LAW «ON THE SECURITY OF THE CRITICAL INFORMATION INFRASTRUCTURE OF THE RUSSIAN FEDERATION» ON OWNERS OF CRITICAL INFORMATION INFRASTRUCTURES

The article deals with topical issues related to the issue of the federal law of July 26, 2017 No 187-FL «On the Security of the Critical Information Infrastructure of the Russian Federation», and also reflects the main aspects of categorizing critical information infrastructure facilities, which is mentioned in the Government Decree of 08.02.2018 No 127 «On approval of the Rules for the categorization of critical information infrastructure of the Russian Federation, as well as a list of indicators of criticality criteria for critical information objects information infrastructure of the Russian Federation and their values», as the article states that such SSDPECA, for what is created and what features should perform.

Keywords: *critical information infrastructure, information security, categorization of objects.*

На сегодняшний день хакерские атаки грозят неприятностями не только владельцам компьютеров, но и промышленным технологическим системам, и информационным системам жизнеобеспечения городов, и других объектов, входящих в критическую информационную инфраструктуру. Последствия этих сбоев могут быть катастрофичны, поэтому в России принят Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», направленный на защиту такой инфраструктуры.

Весь мир сосредоточен на проблеме обеспечения безопасности инфраструктуры и информационных систем. Компании и госструктуры подсчитывают потенциальные убытки, которые могут понести в ситуации, если не будут готовы к внезапному нападению на свои системы. Поэтому тема безопасности в нынешнее время наиболее актуальна, особенно если речь идет об объектах инфраструктуры, от которых напрямую зависит жизнедеятельность целых городов, отдельных регионов, а то и всей страны.

В конце 2016 года в Госдуму был внесен законопроект «О безопасности критической информационной инфраструктуры Российской Федерации». Тема вызвала у специалистов интерес, но оставила массу сомнений относительно возможности реализации законопроекта на практике.

Критическая информационная инфраструктура Российской Федерации – совокупность объектов критической информационной инфраструктуры (КИИ), а также сетей электросвязи, используемых для организации взаимодействия объектов КИИ между собой.

К объектам КИИ можно отнести информационные системы, информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, области здравоохранения, транспорта, связи, кредитно-финансовой сфере, энергетике, топливной промышленности, атомной промышленности, ракетно-космической промышленности, горнодобывающей промышленности, металлургической промышленности и химической промышленности[1].

Процесс принятия законопроекта тянулся очень долго не случайно. Сейчас, после принятия закона, владельцы КИИ обязаны провести ряд технических и информационных мероприятий по защите объектов. Разумеется, это потребует финансовых вложений, причем внушительных (речь идет о критической инфраструктуре). Взламывают КИИ не так уж часто. Однако если инцидент происходит, то последствия бывают весьма плачевными. Последняя крупная кибератака произошла в мае 2017 года.

WannaCry (также известна как WannaCrypt, WCry, WanaCrypt0r2.0 и Wanna Decryptor) — вредоносная программа, сетевой червь и программа-вымогатель денежных средств, поражающая только компьютеры под управлением операционной системы Microsoft Windows. Программа шифрует почти все хранящиеся на компьютере файлы и требует денежный выкуп за их расшифровку. Её массовое распространение началось 12 мая 2017 года — одними из первых были атакованы компьютеры в Испании, а затем и в других странах. Среди них по количеству заражений лидировали Россия, Украина и Индия. В общей сложности, от червя пострадало более 500 тысяч компьютеров, принадлежащих частным лицам, коммерческим организациям и правительственным учреждениям, в более чем 150 странах мира

Приоритет предупреждения компьютерной атаки перед устранением ее последствий – один из основополагающих принципов обеспечения информационной безопасности вообще и безопасности критической инфраструктуры в частности.

Появление новой Доктрины информационной безопасности России было обусловлено тем, что предыдущая версия, утвержденная в 2000 году, утратила силу. За последние 17 лет в стране произошли существенные изменения в части технологического развития в мире в целом и на различных предприятиях в частности. Вместе с тем возросло и число потенциальных угроз. Утверждение подобного документа стало важнейшим этапом для всей отрасли информационной безопасности. Теперь государство рассматривает информационную безопасность как составляющую национальной безопасности. Кроме того, в Доктрине существенно расширен круг сфер, в которых должна обеспечиваться информационная безопасность: здравоохранение, транспорт, связь, энергетика и промышленность. Также особенный акцент сделан на обеспечение информационной безопасности в кредитно-финансовой сфере[2].

Законопроект «О безопасности КИИ», подготовленный в рамках Доктрины, в первую очередь был направлен на регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры РФ в целях ее устойчивого функционирования при проведении компьютерных атак. Он вводит четкое разделение обязанностей по обеспечению безопасности, а также устанавливает полномочия государственных органов в этом вопросе. В проекте оговариваются процедуры государственного контроля КИИ и порядок подготовки и контроля единой сети электросвязи, обеспечивающей функционирование сетей и групп КИИ. Зафиксирована возможность дифференцированных наказаний за нарушение закона – от административной до уголовной ответственности.

К объектам подобной инфраструктуры отнесены информация, информационные системы, телекоммуникационные сети и автоматизированные системы управления технологическими процессами.

Такие системы должны обеспечивать:

- предотвращение неправомерного доступа к информации, обрабатываемой значимыми объектами, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;
- недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимых объектов;

- восстановление функционирования значимых объектов, в том числе за счет создания и хранения резервных копий необходимой для этого информации;
- непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы России.

Согласно приказу ФСТЭК России № 235 от 21.12.2017 г. «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования» субъекты КИИ должны создавать системы безопасности, включающие в себя правовые, организационные и технические меры защиты информации субъектов КИИ.

Данные системы должны обеспечивать устойчивую работоспособность значимых объектов КИИ.

Системы безопасности включают силы обеспечения безопасности значимых объектов КИИ, к которым относятся подразделения субъекта КИИ, обеспечивающие безопасность КИИ, эксплуатацию объектов КИИ и их функционирование.

Системы безопасности должны функционировать согласно организационно-распорядительным документам, разработанным согласно Требованиям, прописанным в федеральном законе «О безопасности критической информационной инфраструктуры Российской Федерации».

Категорирование объектов критической информационной инфраструктуры (КИИ) осуществляется субъектами КИИ в отношении принадлежащих им объектов КИИ. Для присвоения категории создается специальная комиссия. Об этом говорится в Постановлении Правительства от 08.02.2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

Так же в нем регламентируются порядок и сроки категорирования объектов КИИ, перечень критериев значимости объектов КИИ, и показателей для количественной оценки значения критерия.

Для проведения категорирования решением руководителя субъекта критической информационной инфраструктуры создается комиссия по категорированию, в состав которой включаются: руководитель подразделения, работники по ГТ и работники по ГО и ЧС.

Комиссия по категорированию в ходе своей работы:

а) определяет процессы, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры;

б) выявляет наличие критических процессов у субъекта критической информационной инфраструктуры;

в) выявляет объекты критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов, а также готовит предложения для включения в перечень объектов;

г) рассматривает возможные действия нарушителей в отношении объектов критической информационной инфраструктуры, а также иные источники угроз безопасности информации;

д) анализирует угрозы безопасности информации и уязвимости, которые могут привести к возникновению компьютерных инцидентов на объектах критической информационной инфраструктуры;

е) оценивает в соответствии с перечнем показателей критериев значимости масштаб возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры;

ж) устанавливает каждому из объектов критической информационной инфраструктуры одну из категорий значимости либо принимает решение об отсутствии необходимости присвоения им категорий значимости[3].

Исходя из результата работы комиссии объекту КИИ присваивается категория значимости согласно перечню показателей критериев значимости.

Значимость определяется размером ущерба, который будет причинен государству, обществу и владельцу КИИ в случае выхода из строя объекта.

Показатели сгруппированы по пяти типам значимости: социальная, политическая, экономическая, экологическая и значимость для обеспечения обороны страны, безопасности государства и правопорядка. Например, к социальной значимости относится критерий

«Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов)»; к политической – «Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации» и т. д.

Постановлением ограничен срок категорирования после утверждения субъектом КИИ до одного года. Далее в течение пяти рабочих дней необходимо направить перечень объектов в федеральные органы исполнительной власти, уполномоченные в области обеспечения безопасности КИИ.

Комиссия оформляет свое решение по категорированию актом и подписывает его. Руководитель субъекта КИИ утверждает акт и направляет в течение 10 дней данные в органы исполнительной власти, уполномоченные в области обеспечения безопасности КИИ (см. рис.).

Субъект КИИ обязан не реже раза в 5 лет осуществлять пересмотр присвоенной категории значимости в соответствии с Правилами, утвержденными постановлением Правительства № 127 от 08.02.2017 г. Ведь вместе с утверждением ФЗ «О безопасности КИИ» в УК РФ была добавлена новая статья 274.1, которая устанавливает уголовную ответственность должностных лиц субъекта КИИ за несоблюдение установленных правил эксплуатации технических средств объекта КИИ или нарушение порядка доступа к ним вплоть до лишения свободы сроком на 6 лет. Пока данная статья не предусматривает ответственности за невыполнение необходимых мероприятий по обеспечению безопасности объекта КИИ, однако в случае наступления последствий (аварий и чрезвычайных ситуаций, повлекших за собой крупный ущерб) непринятие таких мер подпадает по состав 293 статьи УК РФ «Халатность». Дополнительно следует ожидать внесения изменений в административное законодательство в части определения штрафных санкций для юридических лиц за неисполнение Закона. С большой долей уверенности можно говорить о том, что именно введение существенных денежных штрафов будет стимулировать субъекты КИИ к выполнению требований Закона.

В соответствии с федеральным законом от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» органы государственной власти, государственные корпорации и другие организации, относящиеся к КИИ, должны создать у себя ведомственные или корпоративные центры ГосСОПКА (государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации). Для этого организациям необходимы соответствующие технические решения и высокая экспертиза аналитиков, которая позволит осуществлять мониторинг, анализ и расследование инцидентов, а также выполнять ряд других функций.

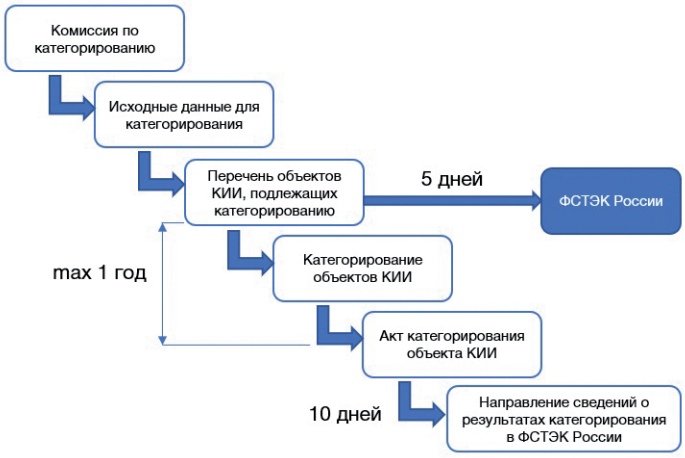


Схема категорирования объектов КИИ

Литература

1. О безопасности критической информационной инфраструктуры Российской Федерации: от 26.07.2017 № 187-ФЗ (последняя редакция) // Консультант Плюс. Законодательство. ВерсияПроф [Электронный ресурс] / АО «Консультант Плюс». – М., 2018.

2. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) // Консультант Плюс. Законодательство. ВерсияПроф [Электронный ресурс] / АО «Консультант Плюс». – М., 2018.

3. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений от 08.02.2018 г. № 127: Постановление Правительства // Консультант Плюс. Законодательство. ВерсияПроф [Электронный ресурс] / АО «Консультант Плюс». – М., 2018.

References

1. On the Security of the Critical Information Infrastructure of the Russian Federation: dated July 26, 2017 No. 187-FL (last version) // Consultant Plus. Legislation. VersionProf [Electronic resource] / JSC Consultant Plus. - M., 2018.

2. The Doctrine of Information Security of the Russian Federation (approved by the Decree of the President of the Russian Federation of December 5, 2016 No. 646) // Consultant Plus. Legislation. VersionProf [Electronic resource] / JSC Consultant Plus. - M., 2018.

3. On the approval of the rules for categorizing the objects of the critical information infrastructure of the Russian Federation, as well as the list of indicators of criteria for the significance of critical information infrastructure facilities of the Russian Federation and their values dated 08.02.2018 No. 127 - Government Decision // Consultant Plus. Legislation. VersionProf [Electronic resource] / JSC Consultant Plus. - M., 2018.

ВАНЦЕВА Ирина Олеговна, магистрант кафедры «Информационные технологии и защита информации» Уральского государственного университета путей сообщения, 620034, г. Екатеринбург, ул. Колмогорова, д. 66. E-mail: east_94@mail.ru

VANTSEVA Irina, Graduate student of Department «Information Technology and Information Security» of the Ural State University of Railway Transport. Bld. 66, Kolmogorova str., Yekaterinburg, 620034. E-mail: east_94@mail.ru

ЗЫРЯНОВА Татьяна Юрьевна, заведующий кафедрой «Информационные технологии и защита информации» Уральского государственного университета путей сообщения, канд. тех. наук. 620034, г. Екатеринбург, ул. Колмогорова, д. 66. E-mail: tzyryanova@usurt.ru

ZYRYANOVA Tatiana, Chief of Department «Information Technology and Information Security» of the Ural State University of Railway Transport. Bld. 66, Kolmogorova str., Yekaterinburg, 620034. E-mail: tzyryanova@usurt.ru

МЕДВЕДЕВА Оксана Олеговна, магистрант кафедры «Информационные технологии и защита информации» Уральского государственного университета путей сообщения, 620034, г. Екатеринбург, ул. Колмогорова, д. 66. E-mail: oks__@mail.ru

MEDVEDEVA Oksana, Graduate student of Department «Information Technology and Information Security» of the Ural State University of Railway Transport. Bld. 66, Kolmogorova str., Yekaterinburg, 620034. E-mail: oks__@mail.ru

УДК 004.056 + 004.7 Вестник УрФО № 1(27) / 2018, с. 77–83

Вотинов М. В.

ТЕОРЕТИЧЕСКИЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ФУНКЦИОНИРОВАНИЯ ПРОМЫШЛЕННЫХ КОМПЛЕКСОВ С ЦЕЛЬЮ УЛУЧШЕНИЯ ИХ ЭКСПЛУАТАЦИОННЫХ ХАРАКТЕРИСТИК В ЧАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Работа посвящена актуальным вопросам обеспечения защиты информации, обрабатываемой в промышленных комплексах на критически важных и потенциально опасных объектах, представляющих повышенную опасность для жизни и здоровья людей и окружающей природной среды. В работе на примере программно-аппаратного комплекса малогабаритной сушильной установки, содержащего в себе не только систему автоматического управления технологическим процессом, но и средства удалённого доступа и мобильного контроля в рамках концепции Промышленного интернета вещей (IIoT), выделены уровни обработки информации, показано определение класса защищённости, и соответствующего набора мер защиты информации, которым должен соответствовать комплекс согласно руководящим документам ФСТЭК России. Представлена реализация определённых мер защиты информации, направленная на повышение общего уровня безопасности технологического процесса.

Ключевые слова*: защита информации, информационные системы, вычислительные сети.*

THEORETICAL ANALYSIS AND STUDY OF THE OPERATION OF INDUSTRIAL COMPLEXES WITH THE AIM OF IMPROVING THEIR PERFORMANCE IN TERMS OF INFORMATION SECURITY

The work is devoted to topical issues of ensuring the protection of information processed in the industrial complexes on the critical and potentially dangerous objects, representing an increased danger to life and health of people and the natural environment. In the example hardware-software complex of small dryer, which contains not only the automatic control system of technological process, but remote access tools and mobile control in the framework of the concept of Industrial Internet of things (IIoT), dedicated levels of information processing, shows the definition of the class of security, and relevant set of information protection measures, which must conform to the complex in accordance with the guiding documents of the FSTEC of Russia. Are the implementation of certain security policies aimed at improving the overall security of the process.

Keywords: *information security, information systems, computer network.*

Введение

С развитием вычислительной техники и технологий все большее количество сфер жизнедеятельности человека подвергается информатизации. Сейчас практически вся информация тем или иным способом хранится и обрабатывается в рамках компьютерных информационных систем с использованием информационных технологий. Мы находимся на пороге времени, когда все больше услуг начинает предоставляться в электронном виде. Стремимся к полной информатизации своей деятельности. Уже невозможно представить отрасль хозяйства, где бы не использовались информационные технологии и информационные системы.

Информатизация общества активно поддерживается и на правительственном уровне. Так, Министерством связи и массовых коммуникаций РФ разработана государственная программа «Информационное общество», которая предполагает, что к 2020 году 85 % населения России будет пользоваться услугами в электронном виде.

Однако развитие информационных технологий порождает вопросы, связанные с защитой информации. Действительно, когда большая часть информации «оцифрована», содержится и обрабатывается в информационных системах, всегда будет существовать круг лиц, заинтересованных в её использовании в своих корыстных целях.

В связи с этим параллельно развитию информационных технологий развивается и система нормативно-правовых документов по обеспечению защиты информации. Система основывается на Конституции Российской Федерации, федеральных законах, нормативной базе органов исполнительной власти, государственных отраслевых стандартах и так далее. В частности, Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» регламентирует права субъекта персональных данных, обязанности оператора системы по обработке персональных данных. Закон РФ от 21 июля 1993 г. № 5485-I «О государственной тайне» регламентирует перечень сведений, составляющих государствен-

ную тайну, защиту государственной тайны, а также контроль и надзор данной сфере.

Вопросы защиты информации охватывают не только конкретные виды информации, но и являются приоритетными при рассмотрении безопасности страны в целом. Так, Указом Президента России от 5 декабря 2016 г. № 646 утверждена доктрина информационной безопасности Российской Федерации, представляющая собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

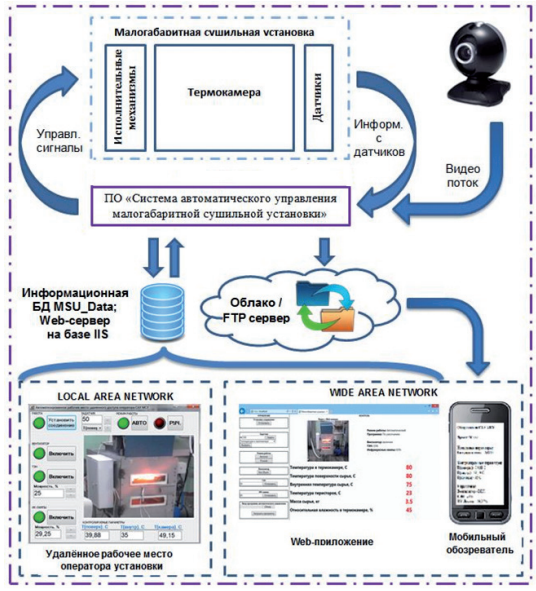
В общем случае обеспечение безопасности представляет собой комплекс мероприятий, начиная от прогнозирования угроз безопасности, их анализа и оценки и заканчивая их выявлением и ликвидацией.

Вместе с тем, помимо классических информационных систем, включающих в себя базу данных и клиентское программное обеспечение, например: автоматизированная система управления кадровыми ресурсами (АСУКР), автоматизированная система управления предприятием (АСУП), сайт в сети интернет, – в которых довольно просто определить вид хранящейся информации и необходимую степень защиты информации, существует отдельный класс систем, до недавнего времени не в полной мере охваченный требованиями по защите информации. Речь пойдёт о промышленных комплексах, в состав которых входят автоматизированные системы управления технологическими процессами.

Следует понимать, что промышленные комплексы также являются источниками информации. Обеспечение информационной безопасности таких комплексов, в зависимости от того, какую важность и опасность представляют они собой для жизни и здоровья людей и окружающей природной среды, является актуальной на сегодняшний день задачей, как и привитие будущим специалистам (студентам и магистрантам) понимания того, что не достаточно построить информационную систему, создать автоматизированную систему управления технологическим процессом, проложить вычислительную сеть, необходимо ещё в полной мере задуматься над вопросами защиты обрабатываемой в них информации.

Описание используемого комплекса

В учебно-экспериментальном цехе Мурманского государственного технического университета функционирует программно-аппаратный комплекс для тепловой обработки рыбного сырья (сушка, вяление, копчение рыбы). Комплекс представлен малогабаритной сушильной установкой [1] и содержит в себе не только систему автоматического управления технологическим процессом, но и оснащён в рамках концепции IIoT современными средствами удалённого доступа и мобильного контроля собственной разработки, позволяющими в режиме реального времени по телекоммуникационным каналам связи отслеживать проводимый технологический процесс [2]. Общая структурная схема комплекса приведена на рисунке.



Информационные потоки программного комплекса

Программная часть комплекса позволяет организовывать удалённый доступ и управление технологическим процессом по локальной сети с использованием программного обеспечения «Удалённое рабочее место оператора установки» (ПО «АРМ»), а также по глобальной сети с использованием Web-приложения. Мониторинг параметров технологического процесса возможен с любого мобильного устройства (мобильные телефоны, планшетные компьютеры и так далее) с использованием разработанного мобильного обозревателя.

Вместе с тем, в составе программной части комплекса находится Web-камера, которая передаёт видео поток во все используемые средства и, тем самым, позволяет визуализировать протекающий технологический процесс находящемуся на удалении операто-

ру-технологу или преподавателю, контролирующему ход выполнения лабораторной работы.

В состав аппаратной части комплекса входит оборудование отечественного производителя автоматики, фирмы «ОВЕН», центробежный вентилятор, инфракрасные лампы, трубчатые электронагреватели, датчики температуры и влажности.

Подробно останавливаться непосредственно на реализации комплекса не будем, отметив только то, что аппаратная и программная части комплекса сведены воедино программным обеспечением «Система автоматического управления малогабаритной сушильной установкой» (ПО «САУ МСУ»). Данное программное обеспечение выполняет функции системы автоматики, обеспечивая управление технологическим процессом с помощью исполнительных механизмов на основании информации с датчиков, а также обеспечивает функционирование средств удалённого доступа и мобильного контроля, работая с информационной базой данных MSU_Data и передавая информацию о технологическом процессе через FTP-сервер на мобильный обозреватель системы. Таким образом, можно с уверенностью сказать, что в составе комплекса функционирует как система автоматического управления, так и классическая информационная система, состоящая из базы данных и клиентских средств удалённого доступа и мобильного контроля.

По представленной схеме функционируют многие промышленные комплексы, взять, к примеру, работающие под управлением TRACE MODE Data Center или использующие для удалённого управления беспроводные системы связи стандарта GSM, выпускаемые фирмами Овен, Siemens, MOXA, TELEOFIS.

Использование средств, обеспечивающих удалённый доступ к промышленным комплексам, управление технологическим процессом или просто его мониторинг, приводит к возникновению рисков утечки информации и негативным последствиям на сложных технологических операциях.

Федеральной службой по техническому и экспортному контролю (ФСТЭК России) принят приказ № 31 от 14 марта 2014 г., утверждающий требования по обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных и потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и окружающей природной среды [3].

Приказ не содержит положений, устанавливающих обязательную аттестацию автоматизированных систем управления производственными и технологическими процессами [4], однако игнорировать его требования крайне не целесообразно.

Хотя малогабаритная сушильная установка и не является критически важным производством, для неё был обеспечен ряд требований в соответствии с руководящими документами ФСТЭК.

Определение мер по защите информации

Системы автоматического управления, обеспечивающие функционирование потенциально опасных производств и технологических процессов относятся к ключевым системам информационной инфраструктуры [4]. Для таких систем мероприятия по обеспечению защиты информации подразумевают определение актуальных угроз безопасности информации, формирование базовой модели угроз и нарушителей, а также определение мер защиты информации.

Нормативные документы, касающиеся ключевых систем информационной инфраструктуры носят закрытый характер и не находятся в общем доступе в сети «Интернет», однако, в состав нашего комплекса входят информационные системы в виде средств удалённого доступа и мобильного контроля. Таким образом, для обеспечения их защиты вполне возможно, по крайней мере, в образовательных целях, пользоваться нормативными документами, регламентирующими обеспечение защиты информационных систем общего пользования.

Что касается мер защиты информации непосредственно систем автоматического управления, то они регламентированы приказом ФСТЭК России № 31 от 14 марта 2014 г. и зависят от класса защищённости. Выделяется три класса защищённости К1-К3. Отнесение программно-аппаратного комплекса к тому или иному классу зависит от уровня значимости обрабатываемой информации.

В малогабаритной сушильной установке можно выделить три уровня обработки информации:

– нижний уровень, на котором обрабатывается информация с датчиков и формируются управляющие сигналы для исполнительных механизмов;

– средний уровень, на котором осуществляется функционирование ПО «САУ МСУ»;

– верхний уровень, на котором осуществляется функционирование средств удалённого доступа и мобильного контроля.

Для определения класса защищённости комплекса необходимо для каждого уровня обработки определить уровень защищённости информации, ориентируясь по оценке возможной степени ущерба для целостности, доступности и конфиденциальности обрабатываемой информации.

Так как технологические процессы, протекающие в малогабаритной сушильной установке, не попадают под определение «критически важных», то для всех свойств безопасности информации были определены низкие степени ущерба, и, как следствие, определён третий, самый низкий уровень значимости информации, обрабатываемой на всех уровнях исследуемого программно-аппаратного комплекса.

Третьему уровню значимости информации соответствует третий класс защищённости системы автоматического управления малогабаритной сушильной установки. Согласно определённому классу защищённости в соответствии с приложением № 2 приказа ФСТЭК России № 31 от 14 марта 2014 г. был выявлен состав мер защиты информации, которые необходимо реализовать для защиты рассматриваемого программно-аппаратного комплекса.

Состав мер защиты информации в системах автоматического управления включает в себя двадцать положений, каждое из которых разбито на несколько пунктов, выбор которых зависит от класса защищённости системы.

Важно понимать, что программно-аппаратный комплекс малогабаритной сушильной установки действует на территории учебно-экспериментального цеха, а его средства удалённого доступа и мобильного контроля отчасти интегрированы в вычислительную сеть университета. Поэтому некоторые меры защиты информации, как то антивирусная защита, обновление базы данных признаков вредоносных компьютерных программ, контроль доступа лиц в помещение цеха изначально были реализованы.

Анализ мер защиты информации заставил серьёзно подойти к вопросам идентификации, аутентификации пользователей, управления доступом к программной части комплекса. В частности, в ПО «САУ МСУ» и ПО «АРМ» были интегрированы механизмы парольной защиты, налажена система рангов доступа, при которой операторы-технологи, студенты и разработчики имеют различные права при работе и обслуживании комплекса. Так, полные права доступа имеют разработчики комплекса, операторы-технологи могут помимо технологического процесса, управлять настройками архивирования информации, студентам доступны только основные функции по ведению технологического процесса.

Доступ к рабочей станции, на которой установлены программные модули системы, также осуществляется с применением политики учётных записей пользователей, позволяя ограничивать их права и возможности при работе в операционной системе, в частности, это позволяет уменьшить риски, связанные с установкой неразрешённого программного обеспечения.

Доступ к управлению технологическим процессом по средствам Web-приложения осуществляется по закрытым каналам связи по протоколу Secure Socket Layer (SSL).

Помимо стандартной регистрации событий, которая осуществляется операционной системой MS Windows, в программной части комплекса реализована регистрация событий безопасности в системе автоматики малогабаритной сушильной установки. Регистрируются возможные случаи отказа датчиков, необоснованное повышение рабочих температур в силовом блоке установки, выход температуры технологического процесса за рамки допустимого коридора. В случае возникновения ошибок происходит срочное информирование персонала, работающего за малогабаритной сушильной установкой и, при необходимости, останов технологического процесса. Регистрация событий необходима для проведения дальнейшего анализа инцидентов, в том числе определения источников и причин возникновения инцидентов, а также оценки их последствий 3.

В целях обеспечения целостности и доступности информации в рамках определённых мер защиты информации осуществляется с помощью бесплатного программного обеспечения xStarter периодическое резервное копирование программных модулей на резервные машинные носители информации.

Немаловажную роль в обеспечении информационной защиты программно-аппаратного комплекса играют организационные

меры. В частности, целесообразно проводить информирование персонала об угрозах безопасности информации, о правилах эксплуатации системы защиты программно-аппаратного комплекса, о возможных нештатных ситуациях и необходимых действиях при их возникновении.

Стоит отметить, что организационные меры по своей значимости не уступают остальным, так как только грамотное поведение персонала в нештатных ситуациях позволяет существенно снизить на потенциально опасных объектах риски, связанные с повышенной опасностью для жизни и здоровья людей и окружающей природной среды.

Заключение

Таким образом, на примере программно-аппаратного комплекса малогабаритной сушильной установки была выполнена реализация мер по защите информации в соответствии с регламентирующими документами ФСТЭК России.

Установка не является критически важным или потенциально опасным объектом, не требует проведения аттестации на соответствие требованиям по защите информации, однако включает, помимо системы автоматического управления, средства удалённого доступа и мобильного контроля, которые делают её уязвимой в плане утечки информации, стороннего вмешательства в технологический процесс, что может привести к негативным последствиям.

Согласно ГОСТ Р 51898-2002 «Аспекты безопасности»: Безопасность – отсутствие недопустимого риска. В этой связи, выполнение мер по защите информации позволило поднять общий уровень безопасности разработанного программно-аппаратного комплекса, снизив вероятность возможных недопустимых рисков, тем самым улучшив его эксплуатационные характеристики.

Практика применения мер по защите информации согласно третьему классу защищённости показала, что поднять уровень информационной безопасности возможно средствами самой операционной системы и используемого программного обеспечения. Вместе с тем, вопросами обеспечения защиты таких комплексов необходимо заниматься ещё на этапе их разработки и внедрения, предусматривая выполнения некоторых мер в рамках уже действующих на предприятиях и организациях системах защиты информации.

Практическая направленность работы состоит во внедрении её результатов не только в технологический, но и в учебный процесс при подготовке студентов и магистрантов по специальности «Автоматизация технологических процессов и производств» для углубления знаний в области защиты разрабатываемых ими систем автоматического управления.

Литература

1. Пат. 135234 Рос. Федерация, МПК A 23 B 4/03. Малогабаритная сушильная установка / Вотинов М. В. ; заявитель и патентообладатель ФГОУВПО «Мурм. гос. техн. ун-т». – № 2013132112/13 ; заявл. 10.07.13 ; опубл. 10.12.13, Бюл. № 34. – 2 с. : ил.

2. Вотинов М.В. Оснащение систем автоматического управления современными информационными средствами удалённого доступа и мобильного контроля // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2017. – Т. 17, № 2. – С. 141–148.

3. Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

4. Информационное сообщение ФСТЭК России от 25.07.2014 № 240/22/2748 «По вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры в связи с изданием приказа ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

References

1. Pat. 135234 Ros. Federaciya, MPK A 23 V 4/03. Malogabaritnaya sushil'naya ustanovka / Votinov M. V. ; zayavitel' i patentoobladatel' FGOUVPO «Murm. gos. tekhn. un-t». – № 2013132112/13 ; zayavl. 10.07.13 ; opubl. 10.12.13, Byul. № 34. – 2 s. : il.

2. Votinov M.V. Osnashchenie sistem avtomaticheskogo upravleniya sovremennymi informacionnymi sredstvami udalyonnogo dostupa i mobil'nogo kontrolya: Vestnik YUUrGU. Seriya «Komp'yuternye tekhnologii, upravlenie, radioehlektronika». – 2017. – T. 17, № 2. – S. 141–148.

3. Prikaz FSTEC Rossii ot 14.03.2014 № 31 «Ob utverzhdenii Trebovanij k obespecheniyu zashchity informacii v avtomatizirovannyh sistemah upravleniya proizvodstvennymi i tekhnologicheskimi processami na kriticheski vazhnyh ob»ektah, potencial'no opasnyh ob»ektah, a takzhe ob»ektah, predstavlyayushchih povyshennuyu opasnost' dlya zhizni i zdorov'ya lyudej i dlya okruzhayushchej prirodnoj sredy» .

4. Informacionnoe soobshchenie FSTEC Rossii ot 25.07.2014 № 240/22/2748 «Po voprosam obespecheniya bezopasnosti informacii v klyuchevyh sistemah informacionnoj infrastruktury v svyazi s izdaniem prikaza FSTEC Rossii ot 14 marta 2014 g. № 31 «Ob utverzhdenii trebovanij k obespecheniyu zashchity informacii v avtomatizirovannyh sistemah upravleniya proizvodstvennymi i tekhnologicheskimi processami na kriticheski vazhnyh ob»ektah, potencial'no opasnyh ob»ektah, a takzhe ob»ektah, predstavlyayushchih povyshennuyu opasnost' dlya zhizni i zdorov'ya lyudej i dlya okruzhayushchej prirodnoj sredy».

ВОТИНОВ Максим Валерьевич, ФГБОУ ВО «Мурманский государственный технический университет», доцент кафедры автоматики и вычислительной техники, кандидат технических наук. 183010, г. Мурманск, ул. Спортивная, 13. E-mail: votinovmv@yandex.ru

VOTINOV Maksim, FSEI HE «Murmansk state technical university», docent of department of Automatic and Computer Engineering, PhD. 183010, Murmansk, Sportivnaya street, 13. E-mail: votinovmv@yandex.ru

ТРЕБОВАНИЯ К СТАТЬЯМ, ПРЕДСТАВЛЯЕМЫМ К ПУБЛИКАЦИИ В ЖУРНАЛЕ

Объем статьи не должен превышать 40 тыс. знаков, включая пробелы, и не может быть меньше 5 страниц. Статья набирается в текстовом редакторе Microsoft Word в формате *.rtf шрифтом Times New Roman, размером 14 пунктов, в полуторном интервале. Отступ красной строки: в тексте — 10 мм, в затекстовых примечаниях (концевых сносках) отступы и выступы строк не ставятся. Точное количество знаков можно определить через меню текстового редактора Microsoft Word (Сервис — Статистика — Учитывать все сноски).

Параметры документа: верхнее и нижнее поле — 20 мм, правое — 15 мм, левое — 30 мм.

В начале статьи помещаются: инициалы и фамилия автора (авторов), название статьи, **аннотация** на русском языке объемом **не менее 700 знаков или 10 строк,** ниже отдельной строкой — ключевые слова. **Ключевые слова** приводятся в именительном падеже в количестве до десяти слов. Инициалы и фамилия автора (авторов) дублируются транслитерацией. **Должны быть переведены на английский язык название статьи, аннотация, ключевые слова.**

УДК
ББК

ОБРАЗЕЦ

А. А. Первый, Б. Б. Второй, В. В. Третий

НАЗВАНИЕ СТАТЬИ, ОТРАЖАЮЩЕЕ ЕЕ НАУЧНОЕ СОДЕРЖАНИЕ, ДЛИНОЙ НЕ БОЛЕЕ 12—15 СЛОВ

Аннотация набирается одним абзацем, отражает научное содержание статьи, содержит сведения о решаемой задаче, методах решения, результатах и выводах. Аннотация не содержит ссылок на рисунки, формулы, литературу и источники финансирования. Рекомендуемый объем аннотации — около 50 слов, максимальный — не более 500 знаков (включая пробелы).

Ключевые слова: список из нескольких ключевых слов или словосочетаний, которые характеризуют Вашу работу.

Рисунки

Вставляются в документ целиком (не ссылки). Рекомендуются черно-белые рисунки с разрешением от 300 до 600 dpi. Подрисуночная подпись формируется как надпись («Вставка», затем «Надпись», без линий и заливки). Надпись и рисунок затем группируются, и устанавливается режим обтекания объекта «вокруг рамки». Размер надписей на рисунках и размер подрисуночных подписей должен соответствовать шрифту Times New Roman, 8 pt, полужирный. Точка в конце подрисуночной подписи не ставится. На все рисунки в тексте должны быть ссылки.

Все разделительные линии, указатели, оси и линии на графиках и рисунках должны иметь толщину не менее 0,5 pt и черный цвет. Эти рекомендации касаются всех графических объектов и объясняются ограниченной разрешающей способностью печатного оборудования.

Формулы

Набираются со следующими установками: стиль математический (цифры, функции и текст — прямой шрифт, переменные — курсив), основной шрифт — Times New Roman 11 pt, показатели степени 71 % и 58 %. Выключенные формулы должны быть выровнены по центру. Формулы, на которые есть ссылка в тексте, необходимо пронумеровать (сплошная нумерация). Расшифровка обозначений, принятых в формуле, производится в порядке их использования в формуле. Использование букв кириллицы в формулах не рекомендуется.

Таблицы

Создавайте таблицы, используя возможности редактора MS Word или Excel. Над таблицей пишется слово «Таблица», Times New Roman, 10 pt, полужирный, затем пробел и ее номер, выравнивание по правому краю таблицы. Далее без абзацного отступа следует таблица. На все таблицы в тексте должны быть ссылки (например, табл. 1).

Примечания

Источники располагаются в порядке цитирования и оформляются по ГОСТ 7.05-2008.

Статья публикуется впервые
Подпись, дата

В конце статьи перед данными об авторе должна быть надпись *«Статья публикуется впервые»,* ставится дата и авторучкой подпись автора (авторов). При пересылке статьи электронной почтой подпись автора сканируется в черно-белом режиме, сохраняется в формате *.tif или *.jpg и вставляется в документ ниже затекстовых сносок. (Либо сканируется последняя страница статьи с подписью и высылается по электронной почте отдельным файлом.)

Обязательно для заполнения: в конце статьи (в одном файле) на русском языке помещаются сведения об авторе (авторах) — полностью имя, отчество, фамилия, затем ученая степень, ученое звание, должность, кафедра, вуз (или организация, в которой работает автор); рабочий адрес вуза или организации (полные – включая название, город и страну – адресные сведения вместе с почтовым индексом, указывать правильное полное название организации, желательно – его официально принятый английский вариант), электронный адрес и контактные телефоны. **Эти данные об авторе должны быть переведены на английский язык.**

Для рассмотрения вопроса о публикации статьи в редакцию журнала необходимо выслать на электронную почту:

1) рукопись статьи, подписанную на последней странице всеми авторами. В рукописи должны быть полные сведения об авторах;

2) в случае, если статья имеет рецензию и заверена печатью, ее оригинал необходимо отправить в редакцию и по электронной почте в отсканированном виде с обязательным указанием контактов рецензента;

3) на статью необходимо выслать экспертное заключение о возможности открытого опубликования (образцы: заключение от руководителя эксперта или заключение от экспертной комиссии.

Библиографические ссылки

Цитируемая в статье литература приводится в виде списка в конце текста. В тексте в квадратных скобках дается ссылка на порядковый номер списка (ГОСТ Р 7.0.5.-2008). Полный текст ГОСТа размещен на официальном сайте Федерального агентства по техническому регулированию и метрологии Авторские примечания (не являющиеся используемой литературой или ссылкой на источник) размещаются в постраничных сносках.

Ниже приводятся образцы оформления сносок:

а) на монографии:

[1] Белова М. С., Кинсбурская В. А., Ялбулганова А. А. Налоговый контроль и ответственность: анализ законодательства, административной и судебной практики / под ред. А. А. Ялбулганова.— М. : Знание, 2008.— С. 12.

б) на статьи из сборников:

[1] Клишина М. А. Новое в порядке составления проекта бюджета // Финансовое право России: актуальные проблемы / под ред. А. А. Ялбулганова.— М., 2007.— С. 101.

в) статьи из журналов и продолжающихся изданий:

[1] Глушко Е. К. Административно-правовая природа государственных корпораций // Реформы и право.— 2008.— № 3.— С. 38—43.

г) авторефераты диссертаций:

[1] Стрижова О. А. Правовое регулирование таможенной стоимости : автореф. дис. … канд. юрид. наук.— М., 2008.— С. 7.

д) интернет-страницы:

Противодействие коррупционным правонарушениям // Юридическая Россия: федеральный правовой портал. URL: http://law.edu.ru/news/news.asp?newsID=12954 (дата обращения: 08.01.2009).

В редакцию журнала статья передается качественно по электронной почте одним файлом (название файла — фамилия автора). Тема электронного письма: Вестник УрФО. Безопасность в информационной сфере.

Отправляемая статья должна быть вычитана автором; устранены все грамматические, пунктуационные, синтаксические ошибки, неточности; выверены все юридические и научные термины. За ошибки и неточности научного и фактического характера ответственность несет автор (авторы) статьи.

Поступившие в редакцию материалы возврату не подлежат.

Материалы к публикации отправлять по адресу E-mail: urvest@mail.ru в редакцию журнала «Вестник УрФО. Безопасность в информационной сфере».

Или по почте по адресу: Россия, 454080, г. Челябинск, пр. им. Ленина, д. 76, ЮУрГУ, Издательский центр.

ВЕСТНИК УрФО
Безопасность в информационной сфере № 1(27) / 2018

Дата выхода в свет 31.03.2018. Формат 70×108 1/16. Печать цифровая.
Усл.-печ. л. 7,70. Тираж 100 экз. Заказ 394/ 631.
Цена свободная.

Отпечатано в типографии Издательского центра ЮУрГУ.
454080, г. Челябинск, пр. им. В. И. Ленина, 76.

Bulletin of the Ural Federal District
Security in the Sphere of Information No. 1(27) / 2018

Date of publication of the 30.03.2018. Format 70×108 1/16. Screen printing.
Conventional printed sheet 7,70. Circulation – 100 issues. Order 394/ 631. Open price.

Printed in the printing house of the Publishing Center of SUSU.
76, Lenina Str., Chelyabinsk, 454080